IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier

A review of methods to study resilience of complex engineering and engineered systems

S. NEDA NAGHSHBANDI[1], LIZ VARGA[1], ALAN PURVIS[2], RICHARD MCWILLIAM[3], EDMONDO MINISCI[4], MASSIMILIANO VASILE[4], MATTHIAS TROFFAES[2], TABASSOM SEDIGHI[5], WEISI GUO[6], ED MANLEY[7], DAVID H. JONES.[8]

[1]S. N. Naghshbandi and L. Varga are with the Department of Civil, Environmental & Geomatic Engineering, UCL, UK, (e-mail: neda.naghshbandi@ucl.ac.uk, l.varga@ucl.ac.uk).
[2]A. Purvis, R. McWilliam, and M. Troffaes are with the Department of Engineering, University of Durham, UK, (e-mail:alan.purvis@durham.ac.uk).
[3]IBEX Innovations Ltd., Sedgefield, UK.
[4]E. Minisci and M. Vasile are with the Department of Mechanical and Aerospace Engineering, University of Strathclyde, UK.
[5]T. Sedighi is with the Centre for Environment and Agricultural Informatics, Cranfield University, UK.
[6]W. Guo is with the Centre for Autonomous and Cyberphysical Systems, University of Cranfield, UK.
[7]E. Manley is with the School of Geography and Leeds Institute for Data Analytics (LIDA), University of Leeds, UK.
[8]David H. Jones is with Neptec UK, Oxfordshire, UK

Corresponding author: S. N. Naghshbandi and L. Varga (e-mail: neda.naghshbandi@ucl.ac.uk, l.varga@ucl.ac.uk).

The authors acknowledge funding from EPSRC ENCORE Network+ EP/N010019/1 which supported many of the contributors.

ABSTRACT Uncertainty and interconnectedness in complex engineering and engineered systems such as power-grids and telecommunication networks are sources of vulnerability compromising the resilience of these systems. Conditions of uncertainty and interconnectedness change over time and depend on emerging socio-technical contexts, thus conventional methods which can conduct normative, descriptive and prescriptive assessment of complex engineering and engineered systems resilience are limited. This paper brings together contributions of experts in complex engineering and engineered systems who have identified six methods, three each for uncertainty and interconnectedness, which form the foundational methods for knowing complex engineering and engineered systems resilience. The paper has reviewed how these methods contribute to overcoming uncertainty or interconnectedness and how they are implemented using case studies in order to illustrate essential approaches to enhancing resilience. It is hoped that this approach will allow the subject to be quantified and best practice standards to develop.

INDEX TERMS Resilience, reliability, robustness, interconnectedness, quantification, case studies.

I. INTRODUCTION

NEW challenges to the resilience of complex engineering and engineered systems (CEES) have been emerging due to the development of highly interactive systems, such as nuclear power plants, power-grids, spacecraft, telecommunication networks, health-care delivery, along with multi-level supply chain systems. Conventional methods of probabilistic modelling and quantification of well-recognised system failure scenarios fail to deal with unanticipated failure modes of complex engineered systems and their recovery options.

CEES defines a holistic system, since an engineered system requires an engineering system. An engineering system includes the set of processes and resources that produce a technical result, whilst an engineered system is a collection of components with specific characteristics which is the outcome of an engineering activity [1]. Systems' resilience is achieved by the capability of the system to sustain system functionality in different conditions and deal with uncertainties caused by natural hazards or human interventions. It is necessary to understand and assess uncertainty and interconnectedness within CEES to provide optimal resilient design and control solutions that can be trusted by society.

In the field of engineering resilience generally refers to the system's capability to bounce back from disruption, restoring some degree of before-shock performance, and exceeding it after recovery is desirable [2]. Most resilience definitions centre on uncertainty quantification, risk management and adaptation [3]. The scope of a resilient CEES is therefore to be able to prepare itself for an emergent situation by: increasing system's awareness, determining weak nodes and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

components by monitoring them; predicting the possibility of failure by monitoring key points; being robust; exploiting redundancy; recovering functionality to fulfil system objective; and learning to improve future resilience.

Designing a resilient CEES is a significant challenge as there is a high level of interconnectedness between systems, as each belongs to a system of systems, constraining the value of adopting a traditional approach of assessing a system's resilience in isolation. Isolated assessment means to consider a restricted set of predetermined parameters and conditions, which fails to take account of the system's endless need to respond to changing needs and related adaptation and evolution processes over its entire life span. Coupled interdependencies between system components and among systems increase their complexity, and make resilience much more difficult to assess. Therefore, the impact on resilience of interdependencies, emergence, and other CEES characteristics should be understood using a complexity science framework which exposes the need for appropriate tools [1] . This supports the need to establish alternative methodologies for assessing a system's resilience, as traditional methods cannot address these challenges. Resilience has attracted significant attention in non-engineering academic domain such as ecology, psychology, economics and organisational science in recent years. Yet in complex engineering and engineered systems, most methods are merely descriptive statistics which are used after a disruptive event rather than methods that address uncertainty and interconnectedness of modern engineering solutions embedded in socio-technical systems [4, 5].

A growing community of interdisciplinary scholars, under the umbrella term of engineering systems research, are striving to provide a rigorous set of tools and methods to design and predict the behaviour of such large socio-technical complex systems [5]. Driven by the tenets of systems and complexity thinking, the engineering systems (ES) themes of interest to scholars are aspects of system interconnectedness, structure or architecture [6] and the influence of uncertainties [7, 8].

Addressing these issues of interconnectedness and uncertainties are the topic of the emerging domain on ES resilience. The construct of ES resilience is a measure of a system's preparedness toward known and unknown threats. Although ES resilience is characterised as an essential functional requirement of commissioned systems, resilience as a concept is still an evolving interdisciplinary domain that suffers from a considerable degree of taxonomical and methodological discrepancy. This is not least because the resilience of an ES is dynamic and changes over its functional life span, being influenced by a multitude of parallel, complex and dynamic interactions, both with elements located within and outside the system.

An apt ES resilience method should be able to provide a theoretical and methodological basis to account for interconnectedness and uncertainties that a system might experience over its functional life time. This necessitates the use of methodological pluralism to unpack the tensions in different scenarios originating out of the coupling of embedded and nested ES. Responding to these challenges and with an intention to contribute to the emerging field of complex ES resilience, a team of interdisciplinary experts joined efforts for this paper to frame the scope, methods and future directions of this domain.

The purpose of this paper is to introduce a set of methodological alternatives available in literature for conducting a normative, descriptive and prescriptive assessment of complex ES resilience, addressing the two primary issues of uncertainty and interconnectedness. This paper responds to these issues by providing six methods organised as follows: 2. Methods for taking uncertainties into account; 2.1 The Bayesian Network for quantifying uncertainty; 2.2 Robust Bayesian modelling for severe uncertainty; 2.3 Multidisciplinary Design Optimisation under uncertainty; 3. Methods for modelling complex interactions; 3.1 Resilience of networked systems; 3.2 Convergent Cellular Automata: theory and application to resilient systems; 3.3 Agent-Based Modelling for complex interactions.

Each of the six methods is described in the context of ES resilience, and provides at least one case study, with a critical assessment of benefits and limitations. The authors do not suggest that an exhaustive list of methods is presented. Instead the objective of the paper is to introduce the readers to the methodologies that can serve as a good starting point to study ES resilience.

II. METHODS FOR TAKING UNCERTAINTIES INTO ACCOUNT

Being embedded into system of systems, the modern engineering system behaviours go beyond their unitary identity into realm of complex and emergent behaviours that are increasingly difficult to model or analyse. A set of tools, categorized under uncertainty quantification use probability driven methods to analyse individual component and system behaviours originating from multiple interactions and system wide complex interdependencies.

A. THE BAYESIAN NETWORK FOR QUANTIFYING UNCERTAINTY

A Bayesian network (BN), also known as belief network, is a directed acyclic graph $G = (V, E)$ which represents a set of vertices (variables/nodes) showed by $V = X_1, X_2, \cdots, X_n$, and a set of edges (casual relations) showed by E that aims to represent conditional probabilities among variables of interest. An outgoing edge from node X_i to X_j indicates a casual relation between these two nodes in which the value of X_j is dependent on the value of X_i. In fact, X_i is the parent node of X_j and X_j is a child node of X_i. In general, three classes of nodes exist in BN: (i) nodes without a child node are called leaf nodes, (ii) nodes without a parent node are called root nodes, and (iii) nodes with parent and child nodes are called intermediate nodes.

The causal relationships among variables of a BN are measured by conditional probability distributions. A condi-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

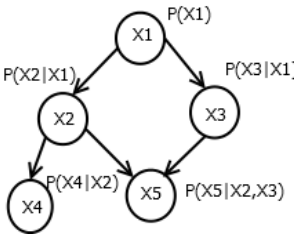


FIGURE 1: Bayesian Network representation with five variables.

tional probability attached to node X_i conditioned on the set of all parents of node X_i, $pa(X_i)$, and is presented by $P(X_i|pa(X_i))$.

Moreover, the full joint probability of all the variables specified in set V is given by,

$$\begin{aligned} P(X_1, \cdots, X_n) &= P(X_1|X_2, X_3, \cdots, X_n) \times \\ &\quad P(X_2|X_3, X_4, \cdots, X_n) \times \cdots \\ &\quad P(X_n - 1|X_n)P(X_n) \\ &= \prod_{i=1}^{n} P(X_i|X_{i+1}, \cdots, X_n). \end{aligned} \quad (1)$$

However, equation (1) can be further simplified with knowledge of conditional interdependency as such, the joint probability distribution of a BN can be written using parent nodes of each node,

$$P(X_1, X_2, \cdots, X_n) = \prod_{i=1}^{n} P(X_i|pa(X_i)). \quad (2)$$

For example, the full joint probability distribution of the BN for Figure 1 consisting of 5 variables X_1, X_2,$\cdots$, X_5 is presented as

$$\begin{aligned} P(X_1, \cdots, X_5) = \quad & P(X_1)P(X_2|X_1)P(X_3|X_1) \times \\ & P(X_4|X_2, X_1)P(X_5|X_2, X_3, X_1) \end{aligned} \quad (3)$$

If we know that node X_4 has exactly one parent, X_2, then the part of joint probability distribution $P(X_4|X_2, X_1)$ can be replaced with $P(X_4|X_2)$, as only X_2 affects the occurrence of X_4. As such, the joint probability distribution of the BN can be written using parent nodes of each node,

$$\begin{aligned} P(X_1, \cdots, X_5) &= P(X_1)P(X_2|X_1)P(X_3|X_1) \times \\ &\quad P(X_4|X_2)P(X_5|X_2, X_3). \end{aligned} \quad (4)$$

This is a key advantage of BN that it requires less parameter than conventional methods and is capable of modeling joint distributions in a compact and economical form.

BNs are constructed based on Bayes' theorem and one of its properties is belief propagation which enables a decision maker to update probabilities of variables $P(X_i)$ after observing the values of some variables. This observed information is called evidence and is denoted by e. For instance in Figure 1, the probability distribution of variable X_3 given the value of all variables except X_3, $(e = X_1, X_2, X_4, X_5)$ is calculated as

$$P(X_3|e) = \frac{P(X_1, X_2, X_3, X_4, X_5)}{\sum_{X_3} P(X_1, X_2, X_4, X_5)}. \quad (5)$$

In real world applications of risk analysis, there are frequently many unknown variables and many distinct pieces of evidence, some of which may be linked [8]. BNs can graphically represent such problems where uncertain variables are represented as nodes, with an edge representing the causal relationship between two nodes. BNs are an excellent tool for computing the posterior probability distribution of unobserved variables conditioned on some variables that have been observed, encoding both quantitative and qualitative information in a conditional probability format.

The ability to model variables of several types (e.g., variables could be Boolean (yes/no), qualitative (low/medium/high), or continuous, among others) is the main property of BN that motivates us to employ it for quantifying of system resilience [7]; [8]; [9]. Consider a large interconnected network like power grids where the failure of a component could possibly trigger the failure of successive components. BNs can be used to quantify the resilience of such systems due to their interconnected structure among their components.

BNs have been deployed in several applications of infrastructure system reliability [10]; [11]; [12]; [13]; [14], but their use in modeling resilience is underdeveloped in the literature. For example, [10] proposed a novel BN model using event log data for analyzing the lateness probability in port logistics. The proposed BN model is constructed by decomposition of a dependency graph that generated from event log data in port management systems. The proposed BN model can then provide valid inference for activity lateness probabilities and also beneficial recommendations to port managers for improving existing activities.

1) Case Study: The resilience of an Inland Water Port, the Port of Catoosa

A case study of the Port of Catoosa, an inland waterway port in the Mississippi River Navigation System located near Tulsa, Oklahoma, is used to illustrate the measurement of resilience using BNs [7]. These ports serve as hubs that connect components of intermodal transportation systems [15].

A BN was employed to quantify the Port of Catoosa's resilience. Natural disasters (e.g., floods, tornados) and hazardous material threats (e.g., fires, explosions, liquid spills) are the primary disruption concerns of decision makers at the Port of Catoosa. As such, natural disasters and hazardous material threats are considered in the BN model as major sources of vulnerability at the port [7]. The graphical model of proposed BN is shown in Figure 2. Three types of variables were used to model the various elements of resilience

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

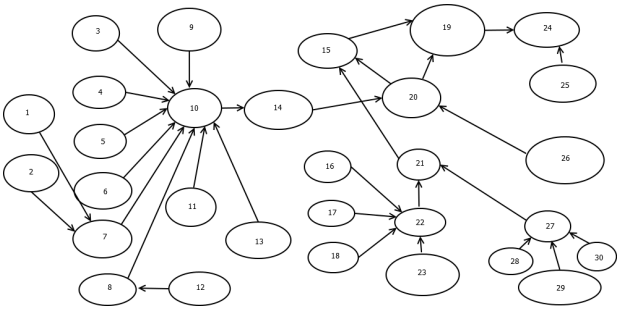


FIGURE 2: The BN model of the inland waterway port system [7]

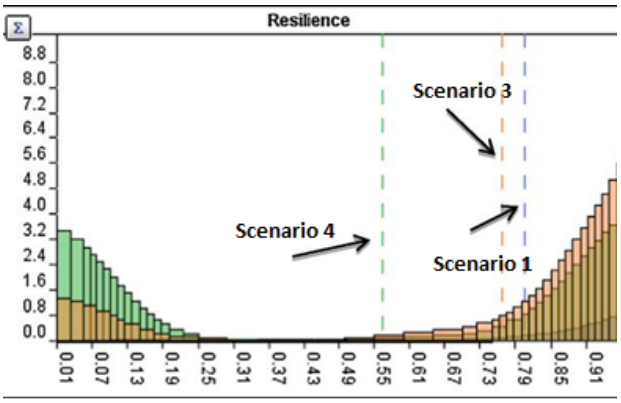


FIGURE 3: Y axis indicates the resilience, and X axis indicates the probability. This figure shows the compression of the probability distributions of the port resilience for different scenarios [7].

capacity, depending on how each are measured: (i) Boolean variables that measure a dichotomous response (true/false, yes/no, on/fail), (ii) qualitative (discrete) variables that measure ordinal categories used for weights of factors contributed to the absorptive, adaptive, and restorative resilience capacities, and (iii) continuous variables that measure random variables with a known probability distribution. Resilience was modeled as the ratio of recoverability to vulnerability and the resilience node is presented in Figure 2 (node 19, see Table 1). In Figure 2 an outgoing edge from Xi to Xj indicates a relationship that value of variable Xj is dependent on the value of Xi variable. For example, the value of the resilience improvements (node 24) is dependent on both the resilience (node 19) and the desired resilience (node 25). For example, if (desired resilience-actual resilience < A), then the value of improved resilience will be computed. Moreover, the reliability (node 8) is dependent on Time to failure (node 12) and is a cause of the adaptive capacity (node 10).

A useful feature of BNs is the ability to propagate the effect of evidence through the network, referred to as "propagation analysis" [16]. Forward propagation implies the propagation of an observed variable and measures its impact on the target variable. If enough evidence of an observation is available, then the observation can be entered into the model, and the probabilities of all unobserved variables can be updated [7].

In this case four decision variables were chosen such that contributions were believed to be significant to the port resilience: maintenance, backup utility system, quick evacuation, and restoration resource. Variables were chosen to fall into each of absorptive (maintenance, backup utility system), adaptive (quick evacuation), and restorative (restoration resource) capacities and four scenarios were performed:

- The first scenario refers to the case when there observation is made that maintenance is not successful.
- The second scenario assumes two failure events of maintenance and restoration resource, leading to a reduction in recovered capacity due to the reduction in restorative capacity which eventually results in a reduction of the port's expected resilience.
- The third scenario simulates the impacts of failures of backup utility system and quick evacuation, and results indicate that the reduction in restorative capacity has a larger adverse impact on resilience.
- The fourth scenario accounts for failure of all four variables, dropping the expected resilience of the port to 55%.

A comparison of the forward propagation analysis scenarios 1, 3, and 4 using BN is illustrated in Figure 3. Figure 3 shows that the distribution of resilience is skewed to the left when adaptive and restorative capacities are reduced, suggesting that adaptive and restorative strategies are important to building resilience.

Consequently, the BN's results show that the resilience capacity of an inland port is related to the three components of absorptive capacity (a means to withstand a disruptive event, or a reduction in vulnerability), adaptive capacity (a means to temporarily adapt to maintain performance), and restorative capacity (a means to restore performance in a long term manner, which with adaptive capacity constitutes recoverability). So, various pre-disaster and post-disaster strategies can improve the three capacities to varying extents, all combining to improve the resilience capacity of the port [7]; [17].

2) Conclusions and limitations

BNs have the ability to combine historical data and expert knowledge, using calculation of prior and posterior conditional probability. BNs provide a rigorous tool for handling risks and decision making under uncertainty based on configuration of a graphical framework. It is a powerful tool for generating risk scenarios.

Many contributions to resilience are qualitative in nature rather than quantitative. Quantifying and assessing resilience from such qualitative variables are difficult when relying on the result of a mathematical optimization model, though such a task is relatively straightforward in a BN (when underlying variables are effectively assessed). Although the BNs also

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

TABLE 1: Nodes of purposed BN in Figure 2. Note that CH and CF stand for Cargo Handling, and Capacity Factor, respectively.

Node	Variable (Variable type)	Node	Variable (Variable type)	Node	Variable (Variable type)
1	On time repair scheduling (Continuous)	11	Skilled labor and management (Boolean)	21	Post disaster strategy (Boolean)
2	Availability of spare equipment(Continuous)	12	Time to failure of port (Continuous)	22	Adaptive capacity (Boolean)
3	Space utilization (Boolean)	13	Extra CH (Boolean)	23	Weights of adaptive CF (Qualitative)
4	System surge protection (Boolean)	14	In-and outbound CH-DOC (Continuous)	24	Resilience improvement (Boolean)
5	Communication and coordination (Boolean)	15	Recovered capacity of CH (Continuous)	25	Desired resilience (Continuous)
6	Backup utility system (Boolean)	16	Repositioning (Boolean)	26	In- and outbound CH-MOC (Continuous)
7	Maintenance (Boolean)	17	Substitution (Boolean)	27	Restorative capacity (Boolean)
8	Reliability (Boolean)	18	Quick evacuation (Boolean)	28	Restoration budget availability (Boolean)
9	Weight of absorptive CF (Qualitative)	19	Resilience (Continuous)	29	Weight of restorative CF (Qualitative)
10	Adaptive capacity (Boolean)	20	lost capacity of CH	30	Restorative resource availability (Boolean)

have been applied in a number of fields, their application to quantifying resilience is still sparse.

Limitations: In spite of the remarkable power and potential to address the dependency between the variables and their conditional probabilities, there are some inherent limitations to BNs:

- Conducting full Bayesian learning is computationally very expensive. This even holds true when the network structure is already given.
- BNs need data and perform poorly with very small data sets.
- Three types of variables: discrete, continuous, and hybrid which includes both discrete and continuous variables can be used in BNs. Although, Dynamic BNs (DBN)s are an extension of BNs that represent temporal changes of variables and edges are used to represent probabilistic dependencies between variables across time (feedback loop).

When the size of data is small, selecting the proper distribution model to describe the data has a notable effect on the quality of the resulting network. Moreover, to remediate this problem (small data set), one of the suggestions is to combine the BN method with the Bayesian optimization method. A Bayesian optimization method can be used to provide more sampling data points from the system's function to improve the data sets used by the BN. Improving the learning process can also reduce the computation time of BN.

B. ROBUST BAYESIAN MODELLING FOR SEVERE UNCERTAINTY

In complex engineering systems, we may be interested in resilience against rare events of which we have only few observations, or we would like to study resilience in systems for which we do not have accurate models, or where the interactions are not yet completely understood. Consequently, in the context of Bayesian analysis (see Section II-A), (i) we may have insufficient data relative to the complexity of the model, leaving a situation where the prior potentially drives a large part of the analysis, (ii) due to lack of expert information and/or lack of experience, it may be hard to identify the prior, (iii) due to model complexity, the full impact of the prior on the posterior may be hard to quantify.

To address problem (ii), non-informative priors have been suggested (see for instance [18] and [19]). Such a prior deems all possibilities equally likely. However, such a statement is still very informative. Therefore, non-informative priors have been strongly criticised by [20], [21], and many others. When there is a lot of data, then the prior has little influence on the posterior, and therefore the prior is not critical. However, when there is little data, it has been argued that it may be better to propagate a set of prior distributions, in order to fully propagate the effects of prior ignorance on the inference. This is called robust Bayesian analysis [22], and allows for a proper treatment of prior ignorance. A problem with this approach is the large computational effort required. However, in many cases, we can work with sets of distributions. Working with sets of distributions also helps us understanding how the prior drives the analysis when data are lacking, particularly in situations where the models are also highly complex (problems (i) and (iii) above).

A wide variety of models have been proposed for dealing with uncertainty and resilience in reliability problems. These include autoregressive time series models, Markov chains [23], Bayesian networks [13], as well as dynamic Bayesian networks [14].

A very powerful yet simple imprecise stochastic model is discussed that allows us to relax stationarity and Markov conditions for dealing with stochastic processes. Then a case study is presented where the set of posterior distributions can be analytically evaluated based on conjugate analysis, and we show how the resulting bounds can be used to quantify resilience of a power network under very weak assumptions about failure and repair times.

Markov chains [24] are commonly used in reliability analysis to quantify resilience of complex engineering systems against system failure, using a variety of risk indices [23]. Informally, a Markov chain is a family $(X_t)_{t\in\mathbb{R}}$ of random variables taking values in a state space S, satisfying:

- For all $s < t$ and all $\delta t > 0$, $X_{t+\delta t}$ is independent of X_s conditional on X_t.
- There is a matrix Q (called rate matrix) such that for small positive $\delta t \simeq 0$:

$$P(X_{t+\delta t} = j | X_t = i) \simeq P(X_t = j | X_t = i) + Q_{ij}\delta t \tag{6}$$

The first condition is called the Markov condition. In the above, infinitesimal notation for convenience was used. Also

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

note that $P(X_t = j|X_t = i)$ is simply 1 if $i = j$ and 0 otherwise. Equation (6) says that the transition probabilities vary slowly, and are independent of time, i.e. the process is stationary.

When using Markov chains to study resilience against system failure, such as the network system that we will consider further, typical issues are that both the Markov assumption and the stationarity assumption are violated, and moreover that only little data is available to estimate parameters. The good news is that we can use probability bounding (i.e. imprecise probability) and robust Bayesian analysis to address all these issues at once. Note that robust Bayesian analysis is by no means restricted to Markov chains, and can be applied to any statistical model, in theory. For example, credal networks are an extension of Bayesian networks to sets of distributions, and have been widely studied and used. We chose to demonstrate robust Bayesian analysis on Markov chains here because they provide a very common model of system reliability.

Imprecise Markov chains model the process $(X_t)_{t\in\mathbb{R}}$ using a set of stochastic processes, subject to the assumption that there is a set $\mathcal{Q}$ of matrices, so that for all t and all histories $x_{s:s<t}$, there is a $Q(t, x_{s:s<t}) \in \mathcal{Q}$ such that:

$$P(X_{t+\delta t} = j|X_t = i, X_{s:s<t} = x_{s:s<t}) \simeq P(X_t = j|X_t = i) + Q_{ij}(t, x_{s:s<t})\delta t \quad (7)$$

The above definition is, for brevity, kept informal; a formal mathematical definition can be found in [25]. Also, note that our choice of rate matrix can fully depend on history and time. Only the set $\mathcal{Q}$ cannot depend on history and time. This model can address issues with stationarity and with the Markov condition. It can also address issues with prior information, as it allows us to use sets of distributions if insufficient information is available.

Even though the processes in the set are far more complex than Markov chains, it turns out that typical quantities of interest can be calculated almost as easily as with standard Markov chains, through a generalisation of the matrix exponential [25]. The next case study demonstrates how this works.

1) Case Study: Power Network Resilience

The case study presented here is based on [26], [27], [28], and [29]; also see [30] and [31].

Consider a power network consisting of two components (say, transmission lines). When both components fail, the system fails, and we want to quantify system resilience against such failure. As model parameters, we have the common-cause failure rate q_2, the 'single-cause' failure rate per component q_1^A and q_1^B, and the repair rates r_A and r_B. Figure 4 depicts the Markov chain for this network. Usually, the failure rates are not observed directly. Instead, we parameterize the system using the alpha-factor model

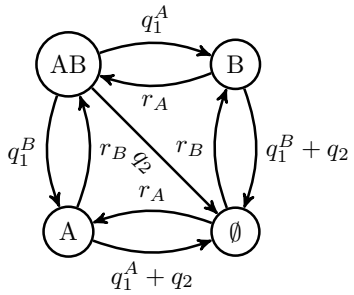


FIGURE 4: Continuous time Markov chain for a 2 component system with common cause failure. Arrows denote possible transitions, and arrow labels denote transition rates. The node AB represents a fully working system, A a system where only A works, B a system where only B works, and $\emptyset$ a system where neither component works.

[32]:

$$q_2 = \frac{\alpha_2}{\alpha_1+2\alpha_2}\left(q_t^A + q_t^B\right), \quad q_1^A = q_t^A - q_2, \quad q_1^B = q_t^B - q_2. \quad (8)$$

This expresses our parameters in terms of observable quantities, namely α_2 which is the fraction of faults due to common cause (note that $\alpha_1 = 1 - \alpha_2$), and q_t^A and q_t^B, which are the failure rates of the components seen separately.

As failure rates are not constant in time, but follow a so-called bathtub curve, there is clear violation of stationarity. Additionally, we have severe uncertainty about the rates themselves, particularly for common cause events. Moreover, the Markov condition is normally violated as well, as repair rates depend on system history, and repair times are not exponentially distributed as predicted by the model. Finally, we have missing covariates. For instance, repair rates depend on operation of the entire power system. Under severe weather, we may see many simultaneous failures, but the number of repair crews may be limited.

Our data consists of nationwide statistics concerning α_2 through observations of consumer disconnections which are typically associated with common cause failures, and also concerning q_t^A and q_t^B through from nationwide statistics about constituents such as average failure rate per kilometer of overhead line. However, regional dependencies are a considerable concern. Therefore, we also use data from the specific network under study, even if this data is only very sparse. Through robust Bayesian analysis, we can use the nationwide statistics to inform our set of prior distributions, which we can then update with the data from the actual network. For the specific data we have available, we find the following posterior intervals on the failure rates (expressed in failures per year):

$$q_1^A \in [0.32, 0.37],\ q_1^B \in [0.32, 0.37],\ q_2 \in [0.19, 0.24]. \quad (9)$$

The repair rates are elicited directly by expert judgment. For instance, if we deem that mean repair times can vary between

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

6 and 12 hours, we get:

$$r_A \in [730, 1460], \quad r_B \in [730, 1460]. \tag{10}$$

The use of imprecise Markov chains means that we allow any time-varying and history dependent repair rate between these bounds.

We can easily construct a set $\mathcal{Q}$ of rate matrices that is compatible with these bounds. We can then evaluate for instance bounds on the limit behaviour:

$$\begin{bmatrix} 9.985\times10^{-1} \\ 2.623\times10^{-4} \\ 2.623\times10^{-4} \\ 6.513\times10^{-5} \end{bmatrix} \leq \lim_{t\to\infty} \begin{bmatrix} P(X_t{=}AB) \\ P(X_t{=}A) \\ P(X_t{=}B) \\ P(X_t{=}\emptyset) \end{bmatrix} \leq \begin{bmatrix} 9.994\times10^{-1} \\ 7.252\times10^{-4} \\ 7.252\times10^{-4} \\ 1.647\times10^{-4} \end{bmatrix}. \tag{11}$$

Similarly, the expected downtime is between 0.57 and 1.44 hours per year, and the expected number of downtime periods is between 0.19 and 0.24 per year. These bounds on risk indices comprise a robust quantification of system resilience under severe uncertainty about system behaviour. This is valuable to decision makers who need to be careful about the impact of model assumptions.

2) Conclusions and Limitations

Authors have discussed how robust Bayesian methods can help quantifying resilience of complex engineering system under severe uncertainty, due to prior ignorance and/or due to lack of data, by using sets of probability distributions. It has been discussed how such sets propagate through models, and imprecise Markov chains was highlighted as a specific example of where such propagation can be done effectively. Authors demonstrated these methods on resilience of a power network.

Authors have concluded that novel mathematical techniques such as imprecise Markov chains enable a much wider class of statistical processes to be used in practice, reducing model discrepancies and improving risk analysis for complex engineering systems. They are useful especially when data is lacking, or when the process itself might not satisfy strong stationarity or Markovian assumptions due to the specific hard to model features of the system itself.

Nevertheless, issues might arise, such as how to get proper probability bounds from data in general, how to incorporate additional covariates if such data is available, and how this analysis can be used in decision making [33], for instance to quantify the trade-off between cost of redundancy and resilience against common-cause failures. Additionally, the utility or loss functions used in decision analysis might be prone to imprecision themselves.

Further challenges arise in complex systems where the likelihood is not from the exponential family, in which case analytical evaluation is impossible, and simulation techniques such as Markov chain Monte Carlo are needed. These techniques are very expensive to run over large sets of priors, especially when the parameter space is very large, and more work is needed in this area.

Future work might focus on Monte Carlo methods for probability bounding, including Markov chain Monte Carlo so data can be adequately incorporated in complex models, similar how to how this is done in modern Bayesian analysis. In addition, elicitation methods for using expert information could be extended to allow experts to express partial probability statements to allow treatment of problems where experts find it hard to express full prior probability distributions.

C. MULTIDISCIPLINARY DESIGN OPTIMISATION UNDER UNCERTAINTY

The Multidisciplinary Design Optimization (MDO) approach, emerged as a new holistic design discipline providing a set of methods and tools to help engineers in the design of system for which the whole is greater than the sum of the parts.

Several MDO methods have been developed to handle the flow of information among the involved disciplines and, then, the complexity of the interactions. The MDO problem in its most general form can be formulated as [34]:

$$\begin{aligned} \min \quad & f_0(\mathbf{x},\mathbf{y}) + \sum_{i=1}^{N} f_i(\mathbf{x}_0,\mathbf{x}_i,\mathbf{y}_i) \\ \text{w.r.t.} \quad & \mathbf{x}, \hat{\mathbf{y}}, \mathbf{y}, \bar{\mathbf{y}} \\ \text{s.t.} \quad & \mathbf{c}_0(\mathbf{x},\mathbf{y}) \geq 0 \\ & \mathbf{c}_i(\mathbf{x}_0,\mathbf{x}_i,\mathbf{y}_i) \geq 0 \qquad \text{for i = 1, ..., N} \\ & c_i^c = \hat{\mathbf{y}}_\mathbf{i} - \mathbf{y}_i = 0 \qquad \text{for i = 1, ..., N} \\ & \mathcal{R}_i(\mathbf{x}_0,\mathbf{x}_i,\hat{\mathbf{y}}_{j\neq i},\mathbf{y}_i,\bar{\mathbf{y}}_i) = 0 \qquad \text{for i = 1, ..., N} \end{aligned} \tag{12}$$

which is known as the "all-at-once" (AAO) problem. In this formulation, N is the number of disciplines, $\mathbf{x}_i$ are the discipline variables ($\mathbf{x}_0$ are variables shared by more than one discipline), $\mathbf{y}_i$ are the coupling variables (output from a single discipline analysis), $\bar{\mathbf{y}}_i$ are the state variables (used only inside one discipline analysis), $\mathbf{x}$ is the concatenation of all the discipline variables, $\mathbf{x} = [\mathbf{x}_0^T, \mathbf{x}_1^T, ..., \mathbf{x}_N^T]^T$, $\mathbf{y}$ is the concatenation of all the coupling variables, $\mathbf{y} = [\mathbf{y}_0^T, \mathbf{y}_1^T, ..., \mathbf{y}_N^T]^T$, f_0 is the global objective function, $\mathbf{c}_0$ are the global constraints, f_i are the discipline objectives, $\mathbf{c}_i$ are the discipline constraints, $\mathbf{c}_i^c$ are the consistency constraints, and $\mathcal{R}_i$ are the discipline analysis constraints. This form of the design optimization problem includes all coupling variables, coupling variable copies, state variables, consistency constraints, and residuals of the governing equations directly in the problem statement.

Uncertainty is an inherent component of complex systems and cannot be avoided. For this reason, researchers have been developing methods and tools to quantify uncertainty and to optimize systems subject to it, by considering that different levels of uncertainty can be present in different steps of the design and can be directly or indirectly related to models, interfaces, and operational conditions. Uncertainty is also added into the process by the fact that several engineers from many disciplines have to interact and exchange information. Moreover, further uncertainty is introduced by the design

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

process itself, and during the design process, uncertainty also changes with time, due to modifications of requirements.

The common formulation of MDO does not necessarily mean that uncertainties are considered during the design process. When this happens, that is better referred to as MDO under Uncertainty (MDOU) [35], which includes 1) the reliability based multidisciplinary design optimisation (RBMDO), 2) the robust multidisciplinary design optimisation (RMDO), or 3) a combination of both. While the aim of RMDO is to optimise the expected performance of the system and reduce at the same time the sensitivity of the optimal result to the expected uncertainties, the RbMDO aims to optimise the expected performance and at the same time keep the violations of the design constraints under acceptable probability thresholds. Clearly, a complete formulation of the problem should consider both robustness and reliability criteria, and then being a robust and reliability based MDO (RRbMDO) problem.

By using the general MDO formulation in (12), the formulation of a generic RRbMDO can be written as in (13),
where, $\mathbf{u}_i$ are the discipline uncertainties ($\mathbf{u}_0$ are uncertainties shared by more than one discipline), $\mathbf{u}$ is the concatenation of all the discipline uncertainties, and $\mathbf{u} = [\mathbf{u}_0^T, \mathbf{u}_1^T, ..., \mathbf{u}_N^T]^T$. In this formulation, each objective function f_i is measured by Ξ_i , which is a measure of either performance criteria or performance variation criteria, for example, the standard deviation or the percentile difference of the performance, and Λ's refer to measures of uncertainty that can rely on probability theory, as well as on evidence theory, possibility theory, interval theory and others.

Resilience can be seen as the ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions. In mathematical terms, this can be seen as the attribute of a dynamical system (or any time dependent system) to be both robust and reliable at the same time. The system resilience can be considered and optimised through modelling of the failure modes and a formulation of the MDOU problem that explicitly takes into account the recovery time.

1) Case study: Space Systems Resilience

There are different sources of uncertainty, which generally can be divided into epistemic and aleatory. Epistemic uncertainties are reducible uncertainties and are due to a lack of knowledge. Aleatory uncertainties are non-reducible uncertainties that depend on the very nature of the phenomenon under investigation. They can generally be captured by well-defined probability distributions as one can apply a frequentist approach. E.g. measurement errors. In this case, the concept of design for resilience in the context of space systems engineering is introduced, and a method to account for imprecision and epistemic uncertainty is proposed. The quantification of robustness and reliability, essential elements of the resilience, in the early stage of the design of a space system is generally affected by uncertainty that is epistemic in nature. As the design evolves from phase A down to phase E, the level of epistemic uncertainty is expected to decrease but still a level of variability can exist in the expected operational conditions and system requirements.

The Evidence Network Models (ENM), a non-directed network of interconnected nodes where each node represents a subsystem with associated epistemic uncertainty on system performance and failure probability, are used to introduce time-dependencies reliability in the modeling of a complex space system. Once the reliability and uncertainty on the performance of the spacecraft are quantified, a design optimisation process is applied to improve resilience and performance.

Given that a generic engineering system is affected by both design parameters $d \in D$ and uncertain parameters $u \in U$, the system can be represented as a network of nodes that share information, where each node is a subsystem and information is shared through the links between subsystems, and the generic objective function can then be defined as:

$$F(\mathbf{d}, \mathbf{u}) = \sum_{i=1}^{N} g_i(\mathbf{d}, \mathbf{u}_i, \mathbf{h}_i(\mathbf{d}, \mathbf{u}_i, \mathbf{u}_{ij})), \qquad (14)$$

where N is the number of subsystems involved, $\mathbf{h}_i(\mathbf{d}, \mathbf{u}_i, \mathbf{u}_{ij})$ is the vector of scalar functions $h_{ij}(\mathbf{d}, \mathbf{u}_i, \mathbf{u}_{ij})$ where $j \in J_i$ and J_i is the set of indexes of nodes connected to the i-th node; $\mathbf{u}_i$ are the uncertain variables of subsystem i not shared with any other subsystem and $\mathbf{u}_{ij}$ are the uncertain variables shared among subsystems i and j.

The test case function used to validate the proposed approach describes the operations of a cube-sat in Low Earth Orbit (LEO). The problem is affected by epistemic uncertainty modelled with the use of Dempster-Shafer theory (DST)[36], and in particular the ENM presented in [37, 38] was used to evaluate the associated Belief and Plausibility curves. The robustness of the solution is guaranteed by the minmax algorithm described in [39, 40, 41]. Finally the resilience of the system during its mission is optimised considering three possible operational states.
The problem is to minimise the mass of the satellite and maximise the amount of data sent back to the ground station. These performance indices depend on design and uncertain parameters. The spacecraft system is modelled as multi-state with a finite number of possible states. The fully or partially functional system can deteriorate or the partially functional system can recover. Once a total failure of the system occurs the system is not able to recover anymore and the satellite is considered lost. The time dependent reliability of a satellite is typically modelled by a Weibull distribution [42, 43]. This work also adopted the Weibull distributions for modelling the reliability, i.e. the transition between both functional states to the failure state.

In this case, better and more extensively described in [44], the sub-system responsible for the recovery from failure is not explicitly modelled, but it would be just an additional element of the multidisciplinary model.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

$$
\begin{aligned}
\min \quad & \Xi_0[f_0(\mathbf{x},\mathbf{u},\mathbf{y})] + \sum_{i=1}^{N} \Xi_i[f_i(\mathbf{x}_0,\mathbf{x}_i,\mathbf{u}_0,\mathbf{u}_i,\mathbf{y}_i)] \\
\text{w.r.t.} \quad & \mathbf{x},\hat{\mathbf{y}},\mathbf{y},\bar{\mathbf{y}} \\
\text{s.t.} \quad & \Lambda_{c,0}[\mathbf{c}_0(\mathbf{x},\mathbf{u},\mathbf{y}) \geq 0] - \Lambda_{Reqc,0} \geq 0 \\
& \Lambda_{c,i}[\mathbf{c}_i(\mathbf{x}_0,\mathbf{x}_i,\mathbf{u}_0,\mathbf{u}_i,\mathbf{y}_i) \geq 0] - \Lambda_{Rec,i} \geq 0 \qquad \text{for i = 1, ..., N} \\
& \Lambda_{cc,i}[\hat{\mathbf{y}}_i(\mathbf{u}) - \mathbf{y}_i(\mathbf{u}) = 0] - \Lambda_{Reqcc,i} \geq 0 \qquad \text{for i = 1, ..., N} \\
& \Lambda_{R,i}[\mathcal{R}_i(\mathbf{x}_0,\mathbf{x}_i,\mathbf{u}_0,\mathbf{u}_i,\hat{\mathbf{y}}_{j\neq i},\mathbf{y}_i,\bar{\mathbf{y}}_i) = 0 - \Lambda_{ReqR,i} \geq 0 \qquad \text{for i = 1, ..., N}
\end{aligned} \tag{13}
$$

2) Conclusions and Limitations

As also emerged during the Defence Academic Pathways Complex Systems Event, held on 4th April 2017, the holistic, model based design management permitted by the MDOU framework will be more and more crucial to design complex systems that have to operate in complex and uncertain environments/conditions, as well as to plan the deployment and use of already designed complex systems.

The reasons why the application of MDOU approaches is still at an initial level are linked to at least two kinds of limitations and technical challenges [45]. One of the key issues to have an efficient MDOU process is the further development of efficient uncertainty propagation techniques in a multidisciplinary environment, as several problems may arise in the propagation of uncertainty among the disciplines. On the other hand, especially at the early stages of the design, the number of uncertainties may be very high and their range can also be relatively broad. In this respect computationally efficient uncertainty quantification techniques must be further developed.

Depending on the nature of uncertainty the literature offers different techniques to address the coupling dilemma [38, 41, 44]. The main difficulty is to devise generally applicable techniques that preserve the required accuracy of the quantification. Model reduction, on the other hand, yields a smaller size problem by identifying and working only with the most important parameters. Another key solution to mitigate the computational complexity of MDOU is the use of surrogate models to create a low cost representation of expensive computational steps. However, building high dimensional surrogates is a challenge in its own right, and again decomposition is instrumental to allow managing complexity and accuracy. In addition, the introduction of approximations, like meta-modelling, brings a further degree of uncertainty that needs to be quantified.

The other challenge in MDOU, often overlooked, is how to correctly model uncertainty. Uncertainty comes in many different flavours. While many techniques exist to treat standard aleatory uncertainty (completely known random processes), the treatment of epistemic uncertainty (lack of knowledge) in MDOU is still a matter of research. Epistemic uncertainty is often not well understood and it has been demonstrated that in many cases it is incorrectly modelled as an aleatory uncertainty with some paradoxical results.

Finally, it is worth mentioning the cultural difficulty in adopting MDOU in the private sector. Overcoming this difficulty requires a considerable cultural shift both in the characterisation of the input uncertainty and in the interpretation of the results. A proper characterisation implies understanding the nature of uncertainty, correctly treating data, understanding the limitations of process and system models, managing subjective probabilities and imprecision and finally understanding the meaning of design solutions. All these aspects add a layer of complexity that is often rejected in favour of simpler, though less meaningful, safety margins. The use of safety margins is also supported by historical data while MDOU often lacks a validation step as design solutions never reach the implementation stage.

III. METHODS FOR MODELLING COMPLEX INTERACTIONS

A. RESILIENCE OF NETWORKED SYSTEMS

The operations of many complex systems involve networking together sub-systems and individual entities. The collective system functionality depends on each component's individual functionality, as well as the coupling dynamics in between. Many of our complex engineering systems exhibit networked dimensions, including electric grids, transportation, telecommunications, water distribution, mail delivery and supply chains. When these networks are large, complex network analysis [46] is not sufficient due to the embedded non-linear dynamics in these networks. To avoid exhaustive simulation studies, it is worth considering complexity and statistical physics methods to better understand networked dynamics and its resilience.

Complexity science has had tremendous success in applying complex network analysis to natural systems. Its track record goes back to the 1970s, where it was shown that a random graph's stability scales inversely proportional to the size and average connectivity of the graph [47]. This demonstrated the risk of growing and connecting systems without thought to its stability. In the past decade, advances have been made to solve challenges in ecology and biology, with examples such as: understanding the stability [48], and robustness of food webs under environmental stressors [49, 50], and universal critical behaviour of biological regulatory networks. In all these examples, topology of the networked interactions has been deemed the dominant

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

force behind behaviour. Unlike their natural world counter parts, many complex engineering systems behave with higher order complexities (e.g. 2+ dimensions). To fully understand networked cascade effects that lead to a loss of resilience, it is important to consider local functional dynamics (e.g. behaviour of a transformer) and the global topology (e.g. structure of the electricity grid) together, and give attention to the sensitivity to demand conditions and the need for tight control.

Definition of resilience and robustness in networks

Resilience is the ability to *bounce back* to a desirable stable behaviour, often after a perturbation that leads it to temporarily be in an undesirable regime. For a given performance metric x at a component (node) i, x_i; we can broadly define a set of desirable and undesirable stable equilibrium points: $\{x_i = x_{i,\mathrm{d}}, \mathrm{d}x_i/\mathrm{d}t = 0\}$ and $\{x_i = x_{i,\mathrm{u}}, \mathrm{d}x_i/\mathrm{d}t = 0\}$ respectively. As these are stable equilibrium points, each node cannot bounce back from $x_{i,\mathrm{u}}$ to $x_{i,\mathrm{d}}$ alone, but through the network's mutualistic coupling, it has the ability to bounce back (e.g. be resilient). A number of metrics can be considered, such as the time to recover from failure as well as the area under the recovery profile (e.g. the *resilience loss triangle*(RLT)) [2].

Robustness is the case when topology dominates dynamics, as is the case in may natural and simple engineering systems, we can simply state that connected nodes will always bounce back and unconnected nodes can never recover from a failure [50]. As such, the binary nature of robustness can be regarded as a special case of the resilience property and more of interest to the macro-state of the network than each node's local functional dynamics. Checking for the robustness of a networked system involves sequential node or edge removal is performed to simulate node or coupling failure, and secondary failures are nodes that become isolated. The sequential node removal process can be random or targeted, and as such, the role of the network topology plays a big part in determining the robustness of the system.

In Figure 5, examples of resilience of a single sub-system and robustness of a networked system (consisting of N sub-systems) are illustrated. In Figure 5a-i, it is shown how a single sub-system with control parameter β can move from a desirable x_{d} (blue) to an undesirable x_{u} (red). In fact, if this moves too far, it becomes unrecoverable (even if we restore β). In Figure 5a-ii,a similar dynamic response, where the performance drops to a recoverable undesirable state and recovers later in time $t = t_1$ is illustrated. Here, the loss of performance over $t_1 - t_0$ is known commonly as the RLT [2]. In Figure 5b-i, many aforementioned sub-systems together are connected via a network and they mutually affect each other. In many cases, they can exhibit a critical behaviour, where unrecoverable functionality in many sub-systems leads to overall collapse of the whole networked system. This appears similar to the case of robustness where one only considers topological failure (Figure 5b-ii), and indeed in many simple dynamical systems, they exhibit similar behaviours [51].

Mean field compression of high dimensional networked resilience dynamics

When explicit functions are given for each node and edge's dynamical behaviour (e.g. ODEs or PDEs), direct analysis and deeper insight is possible. For example, the Markovian behaviour x of any given networked node i can be written as [52]:

$$\frac{\mathrm{d}x_i}{\mathrm{d}t} = f(x_i, \beta) + \sum_{j=1}^{N} a_{ij} g(x_i, x_j), \tag{15}$$

where $f(\cdot)$ is the self-dynamic of node i and $g(\cdot)$ is the coupling dynamic between node i and node j. The connectivity matrix a_{ij} describes the topology of the network. When the dynamics are trivial, the topology dominates overall behaviour and classical complex network analysis applies. When the coupling dynamics are non-trivial, we cannot ignore the high dimensionality of the network (e.g. N-dimensions) and explicit analysis with insight of the governing dynamics is ruled out.

In recent years, *Gao et al.* first proposed a homogeneous mean field approach to compresses the N-dimensional dynamics into a 1-dimensional effective dynamic [52]:

$$\dot{x}_{\mathrm{eff}} = f(x_{\mathrm{eff}}) + \beta_{\mathrm{eff}} \times g(x_{\mathrm{eff}}, x_{\mathrm{eff}}), \tag{16}$$

where the effective dynamic of the whole system x_{eff} is governed by the original local functional behaviours, coupled via a β_{eff} parameter. This parameter represents the role of topology in connecting local dynamics, which is often a combination of weighted degree centrality, but can potentially take on other network centrality measures. This maps the relative importance of self-dynamics $f(\cdot)$ and the role of topology and coupling dynamics $\beta_{\mathrm{eff}} \times g(\cdot)$. Whilst this is the first explicit relationship between dynamics and complex network topology, other approaches have also been used to identify this coupling relationship later on [53].

Here, the collective networked components' dynamics are compressed into an effective average behaviour x_{eff}, which maybe misleading when there is significant heterogeneity in the network. A further innovation by Moutsinas et al., showed that sequential substitution of the homogeneous equilibrium solution x_{eff} back into the original dynamical equation given by Eq.(15) can recover the node level resilience dynamics [51].

1) Case studies: Electricity Grid Cascade Outage, Telecommunication Load Balancing, Rail Transport Resilience

Electricity Grid Cascade Outage: Modeling the dynamical state of electrical transmission networks requires at least 2-dimensional dynamics and a recent framework [54] introduce a framework that takes into account both the event-based nature of cascades and the essentials of the network dynamics.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

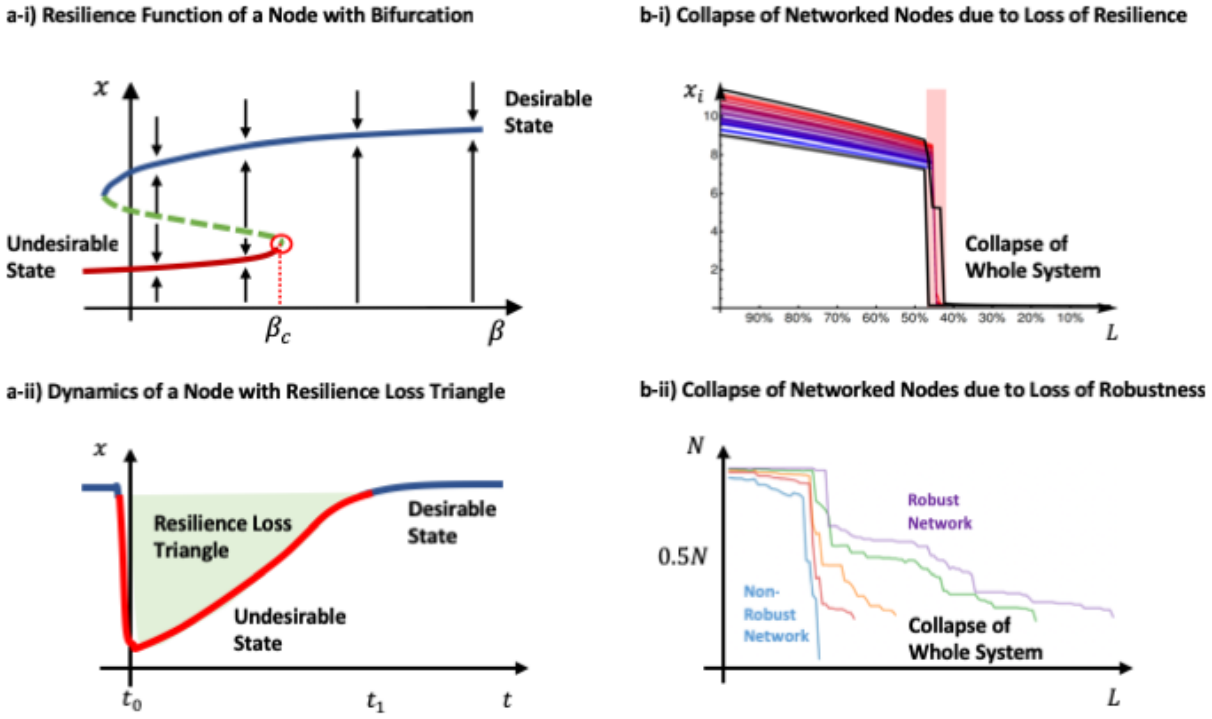


FIGURE 5: Resilience and Robustness in Networked Dynamical Systems: a) a dynamical sub-system, and b) overall networked system.

It was found that transients in the flows of a power grid play a crucial role in the emergence of collective behaviors and propose a forecasting method to identify critical lines and components in advance or during operation. Here, the flow on the line (i, j) with coupling K_{ij} is given by:

$$F_{ij}(t) = K_{ij} \sin\left(\theta_j(t) - \theta_i(t)\right), \tag{17}$$

where θ is the phase angle as a fixed point solution to a power flow analysis. Overload occurs when the flow exceeds a capacity threshold, often set as a tunable threshold of the flow:

$$|F_{ij}(t)| > C_{ij} = \alpha K_{ij}, \tag{18}$$

Where F is the "power flow" $(1/s^2)$, K is coupling strength in power flow $(1/s^2)$, and C is the capacity of the line $(1/s^2)$.

A critical behaviour in unsynchronized nodes can be found as a function of α, demonstrating the importance of tuning capacity in power lines. This has widespread importance in understanding vulnerability power grids to perturbations [55].

Telecommunication Load Balancing: Wireless traffic demand is highly stochastic across spatial and temporal domains. Load is defined as the ratio between traffic demand and capacity: $L(t) = D(t)/C$. An open challenge is whether cascade offloading can cause unstable behaviour, e.g. an endless cycle of offloading between a network of nodes, ultimately degrading the entire network's performance with no benefit. In load balancing dynamics, the self-dynamic of each node tends to wish to move load to a stable equilibrium of $L(t) = 1$, and the coupling offloading dynamic tends to be governed by a difference equation [51]:

$$\frac{\mathrm{d}L_i}{\mathrm{d}t} = \beta(1 - L_i) + \sum_{j=1}^{N} a_{ij}(L_j - L_i). \tag{19}$$

The topology of the network can be accurately modeled using Poisson Point Processes (PPP) and Poisson Cluster Processes (PCP) [56], whereby points are base station nodes and edges are load balancing relations predefined by the operator. The resulting network has a high spatial embeddedness, but in this particular case, is not important to its stability. In the load balancing case of $g(\cdot) \propto (L_j - L_i)$, it can be shown that the stability is governed by the eigenvalues of the Jacobian. In this particular case of load balancing dynamics, the Gershgorin circle theorem determines the location of eigenvalues of the weighted in-degree Laplacian of the graph and it can be shown that the system is always stable, irrespective of the topology. There are a whole host of stability problems in wireless and telecommunication networks, including power control [57], antenna and sleep mode coordination [58].

Rail Transport Resilience: In many cases, explicit dynamics on the nodes and links are not available, but data is available on the flows. In one particular case, the rail

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

transport network's resilience is examined as a function of its multi-modal topology and the flow dynamics along each link between station nodes. In a case study [59], the morning commute journey flow for the Greater London and surrounding counties were examined on all train and overground rail services. For homogeneous linear stability, one might equate resilience with equilibrium points and look at the leading eigenvalue of the Jacobian matrix [47], e.g. instability from leading eigenvalue scales with the size N and average connectivity C of a random graph: $\sim \sqrt{NC}$. Instability in any random graph is proportional to its leading eigenvalue, which is $\propto \sqrt{NC}$, where N is the size of the graph and C is the average connectivity (degree) of the graph. That is to say, larger and more connected random networks are less stable to perturbations. When linear stability is not suitable due to complex dynamics and flow data, many authors have studied system resilience from different perspectives. Some consider the dynamic response (e.g., time to recovery) of the whole system after a specific disruption [7], whilst others use random perturbations to numerically quantify system response. However, such approaches depend strongly on assumptions about the system, such as details of the dynamics or the number of neighbours required for a node to function. In this work we make use instead of recent advances in ecological system analysis to study resilience and robustness, which can be obtained directly from the adjacency matrix (even for weighted and directed networks) and have been found to be good proxies for resilience in ecosystems [48]. The network is thus rearranged into a hierarchical graph, where each trophic level represents its order in the energy transfer of the network (e.g. the highest level takes in most energy and gives out the least). Here, the trophic coherence incoherence q is a proxy metric for the number of unstable feedback loops in the network across different scales, defined as:

$$q = \sqrt{\frac{1}{L}\sum_{ij} a_{ij} x_{ij}^2 - 1}, \tag{20}$$

where a_{ij} is the adjacency matrix, $x_{ij} = s_i - s_j$ is the trophic level difference between levels s_i and s_j, and L is the number of connections in the whole network. The conversion of real data flows to a hierarchical network can be done using either basal node enforcement or flow filtering and this is discussed in [59]. For a network with no feedback, the incoherence is zero; and for a random network, incoherence approaches one.

It was found that the trophic incoherence was highly correlated with both the consumer dissatisfaction and the major delays and cancellations statistics. This shows that incoherent feedback loops cause cascade delays and cancellations that lead to customer dissatisfaction. Compared to potential confounding variables, trophic incoherence contributed more than the size of the network, its robustness, and other operational and network science parameters. This highlights that when explicit dynamics are not available, one can still infer useful resilience metrics from the trophic structure of the network. The researchers go on to identify paths where a service can be increased or decreased to dramatically improve the overall network coherence and hence resilience (details can be found in the paper [59]).

2) Conclusion and limitations

In order to retain tractable understanding of the relationship between dynamics and graph topology, the theoretical challenge going forwards lie in considering more complex dynamical functions. The high-dimensional space of the network domain is not the greatest concern, but high-dimension space of the functional domain, when coupled via a network, is challenging. The major limitations of current Markovian low-dimension space and low-order ODEs (decoupled) is that they can only be applied to a limited set of engineering and ecosystem dynamics, forcing data-driven proxy and statistical methods to play a large role than desired in many networked dynamical systems analysis. Regarding the network properties themselves, extreme variations in heterogeneity in network structure (e.g. strong clustering coefficient in the network) can also reduce the accuracy of mean field analysis.

This leads nicely for researchers to consider data informing uncertainty in the parameters and inputs of the system, which enables the quantification of noise [60], optimal sampling theorems on dynamical graphs [61], and the development of stochastic and data-driven control systems [62].

Further research will focus on topological heterogeneity, non-Markovian dynamics, higher order dynamics, coupling PDEs with ODEs. These are very challenging complexity and non-linear dynamic questions which are essential to faithfully modeling real world engineering systems. Effective model linearisation using Koopman operators to compress nonlinear models into polynomial linear component dynamics can provide a pathway towards tractable complex analysis. And data-driven embedding of appropriate dynamic features can provide a pathway to finding resilience trends in the enriched phase space in absence of tractable models.

B. CONVERGENT CELLULAR AUTOMATA: THEORY AND APPLICATION

A major challenge in creating built-in fault resilience and self-organising capability within complex platforms lies in the merging between effective detection and mitigation via triggered recovery mechanisms. Ideally this should be implemented without incurring major resource overhead or complex coupled-domain behavior. Relevant techniques for fault resilience are summarised in Table 2, arranged broadly in ascending order of complexity. A fault is defined as an undesirable state that may lead to an error state and subsequent malfunction. Fault-driven methods take two fundamental approaches to the problem: fault masking without explicit detection; and fault detection, isolation and recovery (FDIR). By way of example, successful fault masking in electronic systems entails securing error-free operation while the fault condition remains in place and until it either clears naturally (transient) or remains until power off (persistent).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

To address the need for design architectures that support resilient design, one option is to utilitise dedicated reconfigurable platforms, of which the FPGA[1] remains a classic platform in electronic systems [63, 64]. There are however limitations as to what can be achieved using state of the art COTS[2] FPGA and specialised architectures. The necessary target hardware resources, the expected fault scenarios and the required degree of robustness are key factors. When considering complex systems and their integrated subsystems, fault detection represent a complex design tradeoffs; the economic investment required for built-in resilience becoming relatively high in comparison to the functional resources due to design integration and hardware outlay. In this situation, cellular arrays such as cellular automata (CA) are eminently compatible with existing and future configurable platforms and are essentially built upon a compromise between hardware-identical and information redundancies at the fine-grained level. As will be discussed in the following sections, by combining CA with re-configurable information and technology platforms, new possibilities for resilience design strategies, such as self-diagnosis, self-reconfiguration and self-maintenance become available without the specific need for fault detection.

Achieving convergence with Cellular Automata

CA systems are dynamic systems in which space and time are discrete. These tend to be highly distributed systems, composed of large or infinite arrays of cells that use simple programs or sets of rules to determine their next state (e.g. by selecting a colour from a discrete set) according to the current state of their neighbouring cells. The simple behaviour of the local interactions between cells belies the often complicated, chaotic or complex behaviour evident across the entire array. The relationship between the simple behaviour of each cell and resulting emergent properties of the larger array have fascinated mathematicians, computer scientists and biologists since their conception in the 1940's. CA are described by the size and number of dimensions of the array of the cells, the boundary conditions of the array, the set of states each cell can be in, the initial state of each cell, the algorithm used by each cell to determine its next state and the size and shape of the 'neighbourhood' of cells about each cell which form the inputs to this algorithm.

Recent research has focused on whether local rules can be devised such that the CA has desirable emergent properties with practical applications. For instance, an electronic circuit or computer system is an arrangement of individual components. If the emergent behaviour of an automaton is defined as a desired arrangement of components, the correct arrangement will re-emerge in the event that it is corrupted by an external event, leading to the *Convergent* cellular Automata (CCA). However, achieving resilience properties that are applicable to engineering systems is challenging. Barr [71] explored the use of adaptive euler-solvers, Eggenberger [72] tested various unsupervised evolutionary algorithms to derive local rules obeyed by each cell such that specific behaviour is observed across the entire array. More recently, increasingly advanced evolutionary algorithms ([73, 74, 75, 76] have enabled further control.

The CCA is defined here as regular array of identical cells, $c_{x,y}$, each with a corresponding neighbourhood of cells $c_{x-1,y}, c_{x+1,y}, c_{x,y-1}, c_{x,y+1}$. If we restrict the rules each cell uses to determine its next state to be a sum-of-products function of the state of its neighbours, such that the next state of each cell is determined by the formula

$$c_{x,y,t+1} = u.c_{x-1,y}+v.c_{x+1,y}+w.c_{x,y-1}+x.c_{x,y+1}+y.c_{x,y}+z \tag{21}$$

where u, v, w, x, y are constants common to each cell. Converting the CA matrix to a row-major vector $\overline{C_t}$, a transition matrix$A$ can be formed such that the next state of the entire automata can be generated:

$$\overline{C_{t+1}} = A.\overline{C_t} + \overline{D} \tag{22}$$

A and D are the structured arrays of variables u, v, w, x, y and z. For instance, a 2×2 array of cells using the next-state rule (21) would have a the following transition matrix equation

$$\begin{pmatrix} c_{0,0,t+1} \\ c_{0,1,t+1} \\ c_{1,0,t+1} \\ c_{1,1,t+1} \end{pmatrix} = \begin{pmatrix} y & v & x & 0 \\ u & y & 0 & x \\ w & 0 & y & v \\ 0 & w & v & y \end{pmatrix} \begin{pmatrix} c_{0,0,t} \\ c_{0,1,t} \\ c_{1,0,t} \\ c_{1,1,t} \end{pmatrix} + \begin{pmatrix} z \\ z \\ z \\ z \end{pmatrix} \tag{23}$$

By the repeated application of this transition function, the transition from $\mathbf{C}_{t=0}$ to $\mathbf{C}_{t=n}$ (where $n > 0$) becomes

$$\overline{C_{t=1}} = \mathbf{A}(\mathbf{A}\overline{C_0} + \overline{D}) + \overline{D} \tag{24}$$

$$\overline{C_{t=2}} = \mathbf{A}(\mathbf{A}(\mathbf{A}\overline{C_0} + \overline{D}) + \overline{D}) + \overline{D} \tag{25}$$

$$\overline{C_{t=3}} = \mathbf{A}^3\overline{C_0} + \mathbf{A}^2\overline{D} + \mathbf{A}\overline{D} + \overline{D} \tag{26}$$

This can be expanded to form

$$\overline{C_{t=n}} = \mathbf{A}^n\overline{C_0} + \mathbf{A}^{n-1}\overline{D} + \mathbf{A}^{n-2}\overline{D} + ... + \mathbf{A}\overline{D} + \overline{D} \tag{27}$$

Using the geometric series equation this can be simplified to form

$$\overline{C_{t=n}} = \mathbf{A}^n\overline{C_0} + (\frac{\mathbf{I} - \mathbf{A}^n}{\mathbf{I} - \mathbf{A}})\overline{D} \tag{28}$$

If the automata always converges to a single global pattern regardless of its starting state, given sufficient iterations (discrete time-steps of the CA) the final pattern must be independent of the initial pattern. Thus $\mathbf{A}^n$, the coefficient of $\overline{C_0}$, must equal zero. For this to be so, referring to the coefficients of the states of the cells above, below, left and right and of the cell itself respectively, the following must hold: either u or v must equal zero, either w or x must equal zero, z must equal zero. That is, $\mathbf{A}$ must be an upper-diagonal or lower-diagonal matrix.

Given sufficiently large n and a transition matrix that

[1]Field programmable gate array
[2]Commercial off-the-shelf

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

TABLE 2: Concepts of resilience in order of ascending complexity.

Feature	Aim of strategy	Examples
Fine-grained fault masking	Fault masking at lowest design levels; no awareness of fault condition	Redundant elements. See [65];
Self-diagnosis	Determine cause of unexpected faults (possibly cross-domain); intelligent management of resources	Software domain techniques [66]; MEMS integrity test [67]
Self-reconfiguration	Automatic organisation of redundant resources; reallocation	Evolvable hardware [68, 64]
Self-maintenance	Persistent correction of faults during active service to reduce maintenance requirements	Self-maintaining design strategies [69]
Self-preservation	Able to preempt and reduce impact of fault event to reduce impact	Electromechanical shock protection [70].

meets the above criteria, both $\mathbf{A}^n$ and $\mathbf{A}^{n-1}$ of equation (28) will equal zero, and thus $\overline{C}_{t=n} = (\frac{\mathbf{I}}{\mathbf{I}-\mathbf{A}})\overline{D}$. After sufficient iterations, the CA will converge to a final pattern $\overline{C_d}$ according to:

$$(\mathbf{I} - \mathbf{A})\overline{C_d} - \overline{D} = 0 \tag{29}$$

Using the above approach it is possible to design CCA such that a desired pattern will emerge from any initial configuration and will continue to be refreshed in the event of corruption occurring to the configuration. Solving equation (29) for $\mathbf{A}, \overline{C_d}$ given some desired final pattern $\overline{C_d}$, the next-state rule for each cell of the CA can be determined such that the CA always converges to the pattern $\overline{C_d}$. For instance, Figure 8 shows an automata resiliently converging towards a specified complex pattern by virtue of its 140x60 cells obeying the derived rule set.

Convergence as a resilience property

Using the above approach it is possible to design CCA such that a desired pattern will emerge from a defined initial configuration that will continue to be enforced in the event of corruptions. Solving equation (29) for $\mathbf{A}, \overline{C_d}$ given some desired final pattern $\overline{C_d}$, the next-state rule for each cell of the CA can be determined such that the CA always converges to the pattern $\overline{C_d}$. For instance, figure 6 shows a trivial automata resiliently converging towards a simple 2x2 checker flag. Although the initial state shown is an array of zeros convergence is guaranteed for any initial state. The next-state rule used for this automata is $c_{x,y,t+1} = 1 - c_{x-1.y.t} - c_{x,y-1,t}$.

A more detailed illustration of the robustness of convergence is depicted in figure 7. This shows the recovery of a 4x4 pattern after being subjected to a combination of both state randomisation and temporary fault condition.

For both cases, the CCA reconstructs the correct pattern within 9 iterations. The temporary fault takes the form of an incorrect cell coding that is overridden by the CCA rule and is hence restored to the correct state. Boundary cells to the left and above the active area (i.e., outside the white box) influence the coding of rules and states for the given target pattern; boundary cells to the right and below the active area are determined by the current state and, for the

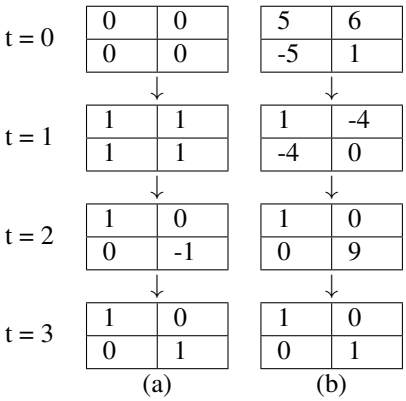


FIGURE 6: Example CA convergence from null (a) and random (b) initial conditions to $\mathbf{C}_d$

example shown, should always display the combination seen in figure 7h. These boundary cells can therefore given an indication of the presence of fault conditions [77]. Figure 8 shows much larger automata converging towards a specified complex pattern by virtue of its 140x60 cells obeying the derived rule set.

1) Case study: Protecting Digital Logic

In order to demonstrate how convergence can be captured a resilience property in engineering systems, we consider the case of electronic systems, whose modular, hierarchical design structure appears a good match to the CCA architecture. The convergent pattern must represent some functional importance. For instance, a data set, logical configuration or machine memory state. For cases in which the required memory for storing CCA next-state rule is smaller than that needed to store the emergent pattern, encoding the memory within a CCA will add resilience to the design. This is most obvious where the data pattern is highly repetitive such as in the checkered flag pattern (figure 6); most complex patters and therefore incur increasing rules and state storage overhead.

For the particular case of protecting digital logic the CCA can be utilised as a coordinating layer that directs configuration functional logic, in turn organising the actual

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

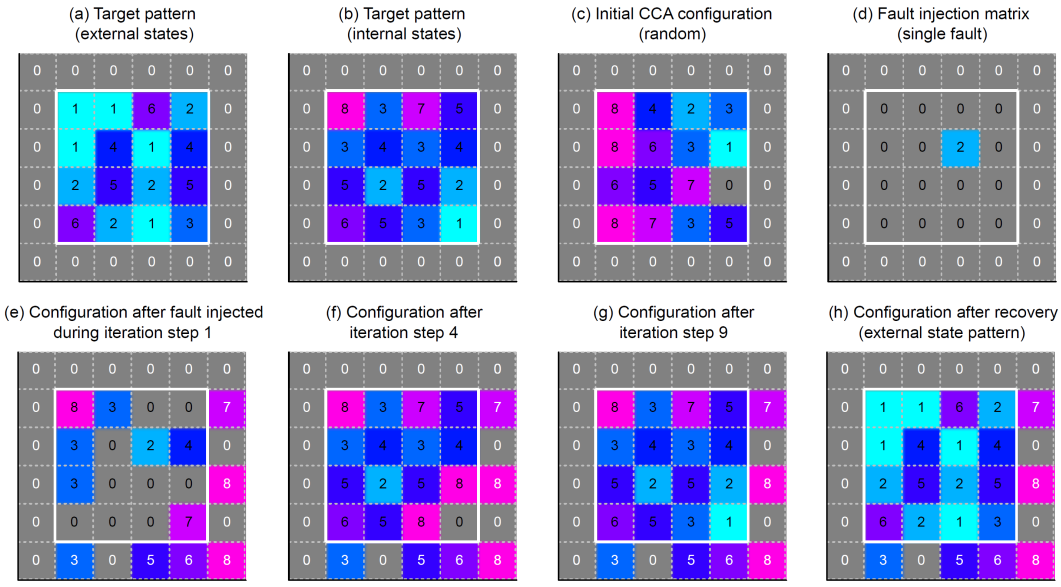


FIGURE 7: Recovery of a 4x4 CCA from a combination of random state initialisaton and a transient fault event persisting during iteration step 1. (a) Target pattern as viewed externally; (b) internal state representation; (c) Random initial state of CCA; (d) location/value of faulty cell state whose state can be overridden by the CCA rule set; (e) internal state after single refresh of cells and including state of faulty cell; (f-g) internal state ofter 4 and 9 iterative updates respectively; (h) resulting CCA pattern after convergence, which matches that seen in (a). The active CCA region is contained within region encircled by white box; boundary cells are denoted by white numbers.

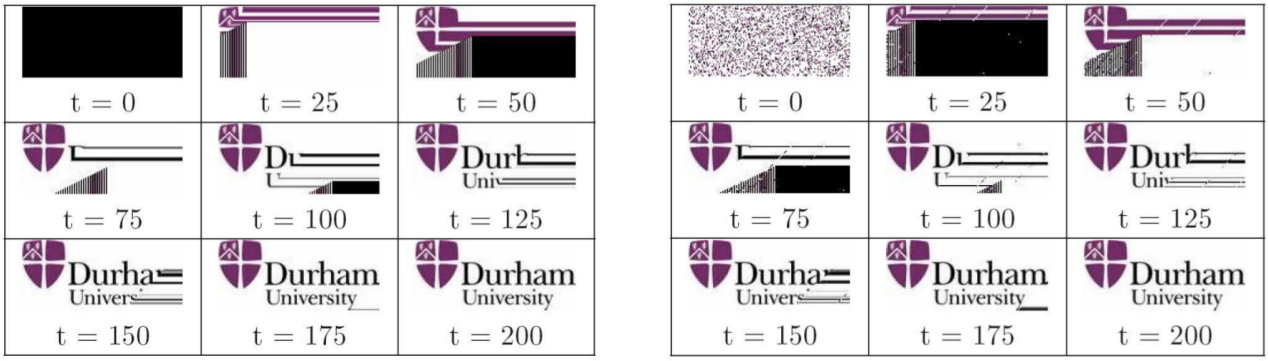


FIGURE 8: A 140×60 CA from null (left), and corrupt (right) initial conditions over 200 iterations.

behvaiour of the logic unit. This concept is illustrated in Figure 9a where the (convergent) cell states are mapped to a set of logic functions. The central idea is to protect logic by exploiting without resorting to fault detection mechanism; instead this duty is performed by virtue of each cell obeying the rule set and, in turn, continually refreshing the correct logic configuration. This offers the advantage of abstracting the resilience level from the (typically) optimised functional logic layer such that the hardware implementation may share either common or distinct resources.

A more detailed breakdown of the approach is illustrated in Figure 9b for a full adder[3]. The 1-bit full-adder circuit is assembled using three logic functions mapped to the states $1, 2, 3$ within the CCA state map, resulting in a compact 4×4 CCA layout though finer-grained solutions are also possible. The choice of granularity is an ongoing area of research and involves several trade-offs concerning efficiency of mapping to the hardware platform and the expected nature of fault and its coverage[4].

To demonstrate the technique, the example configuration of Figure 9b has been extended into a 4×4 CCA design and synthesised into a Xilinx Vertex 5 FPGA platform via VHDL. Further details of the specific implementation and fault injection testing platform can be found in [77]. The test case involved subjecting the CCA configuration to one or more faults that result in the functional logic becoming invalid. This included the extreme case of randomising

[3]The full adder is considered a fundamental building block of common logic cells used in arithmetic logic units.

[4]Fault coverage is discussed at length by Cheatham [64] Parris [63]; it is broadly defined here as the expected region of logic that is typically affected by a fault event. This may occur at the singular gate level or involve multiple gates/cells.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

all CCA cell states. Ordinarily this scenario would require highly complex fault detection logic or else would rely upon complete resetting of the logic with associated down-time. By contrast, the CCA implementation is able to reconfigure the correct logic in all cases without intervention.

2) Conclusions and limitations

CCA present an alternative strategy to conventional fault detection and mitigation mechanisms for increased resilience in complex systems. The approach has been considered in the electronics domain, for which there exists a number established detect-mitigate strategies that have well-established limitations. By encoding convergent behaviour directly into the design fabric, threats appearing in the form of transient upset fault conditions can be addressed without the need for dedicated detection. Further, the core configuration becomes protected by a distributed rule set shared among all cells. The approach is extensible to much larger automata [78] than the example described here, including 3-D automata [79] and automata that converge towards a sequence of patterns [80].

Although this platform presents an attractive proposition for protecting the configuration of reconfigurable platforms, several challenges remain: i) Scalability is important and the associated key factors governing this are choosing of design granularity and the necessary rule/state set size. This is well-understood for smaller CCA but is currently estimated for larger designs. ii) Fault condition: the approach is most effective for transient fault conditions since permanent fault conditions require repairing or replacing the affected resources. This requires changing the configuration by triggering either an alternative rule set or a new set of boundary cell values. An additional challenge is that the underlying fabric must support re-routing between affected and replacement cells. iii) Resource reuse and scalability: for electronic platforms a reasonably fine-grained implementation is possible via FPGAs but high density implementations will require new reconfigurable platforms optimised for CCA resources. Some future directions for CCA are suggested below:

- Scalability: Success of the CCA method depends on deriving efficient rule and state sets that scale favourably for a given pattern size/complexity. The approach adopted in [77] can be used as a model for further investigation.
- Stuck-at fault detection: while the CCA is intrinsically resilient to transitory error events, persistent stuck-at faults may prohibit convergence to the correct state. One potential solution is to exploit CCA cell state redundancy together with observation of boundary cell state values in order to pinpoint the location of the affected cell [77].
- Stuck-at fault mitigation: this requires further research into supporting hardware platforms that not only support CCA architecture, but also allow for dynamic connectivity between the cellular fabric. This is closely related to evolvable hardware platforms [68].
- Alternative applications: aside from protecting critical cell states that represent patterns and data, the CCA method may also be applied to self-assembling hardware whose configuration is then protected in a similar fashion. This requires further investigation of local CCA neighbourhoods and their common boundary cells [80].

C. AGENT-BASED MODELLING FOR COMPLEX INTERACTIONS

Unlike other complexity modelling methodologies described within this paper, agent-based modelling (ABM) offers explicit description of autonomous and heterogeneous facets of a system of interest. Whereas CA demonstrates how spatial proximity and interaction of cells yield models of systemic robustness, ABM relaxes constraints on the representation of entities, allowing for the individual representation of technical objects, subsystems, human decision-makers, and any other relevant individual actors. These entities are individual and autonomous 'agents' in ABMs and allow for the integration of distinct social and technical system components, and therefore enable a more holistic simulation of system resilience with particular relevance to complex engineered and engineering systems (CEES) that accommodate a heterogeneous population of socio-technical components.

Complex systems are characterised by nonlinearity in the relationship between individual actions and exhibited collective behaviour. Through the interdependencies and interactions between components within a complex system, a variety of common characteristics can be observed. Two important forms of this behaviour are emergence – a system trait that cannot be attributed to the actions of an individual component – and self-organisation – the formation of collective structures or behaviours based on cooperation or competition between agents. These two characteristics are observed across a wide variety of contexts, outlined in more detail below. But importantly, complex systems are dynamic in nature, meaning these collective structures can form and dissolve over time, often on the basis of very small perturbations in individual behaviour. It is not unusual to observe phase transitions in complex system behaviour as a result of changes in behaviour of only a relative few components. Complex systems may also be adaptive, meaning that modelled components can have memories, learn and adjust behaviour based on feedback, some following rational rules and others acting stochastically. Learning can potentially maintain or threaten a system held in equilibrium. Finally complex systems can evolve which means that through acquisition of new traits or through access to different resources, parts of the system can mature their capability and we recognise that the system has changed and usually describe it.

Agent-based modelling has emerged as a core methodology in the understanding and simulation of both technical and social components of complex systems within a single integrated simulation. Through representation of individual agents and their interactions with each other and with CEES products and systems, ABMs replicate the microscopic be-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

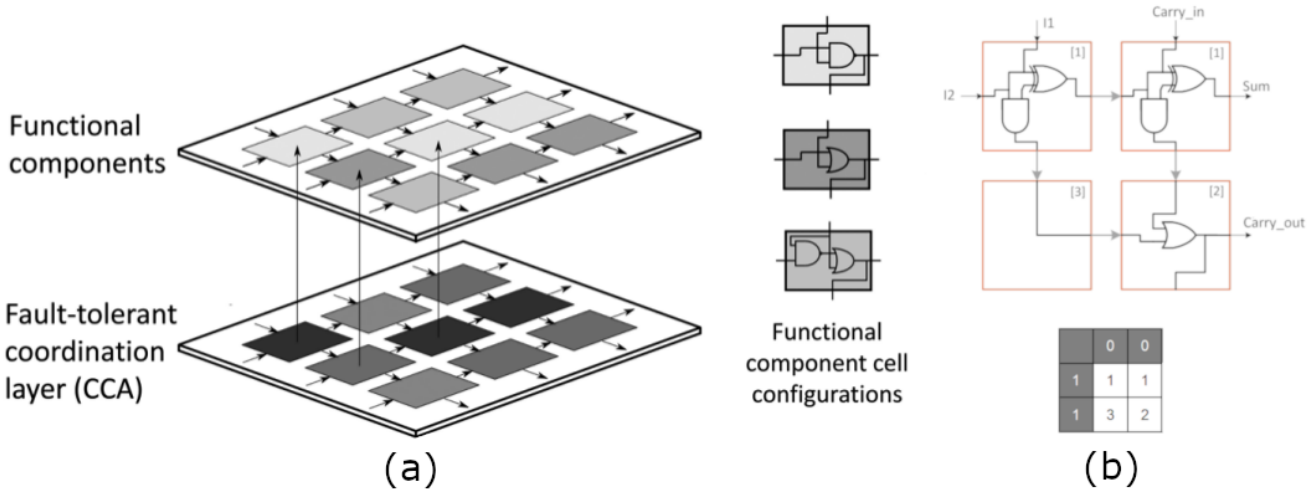


FIGURE 9: Illustration of resilient logic implemented using a CCA coordination layer and functional logic layer. (a) arrangement of coordination and function layers along with example component cell configurations; (b) Illustrative example configuration for combinatorial logic adder with simple CCA coordination pattern.

haviours that lead to emergence (e.g. congestion), self-organisation (e.g. autonomous re-routing), evolution (novel forms or topologies), and other properties of complex systems (e.g. repeated patterns/waves). An ABM allows us to test the conditions under which these properties arise and dissipate in response to changes in internal or external conditions. Within this context, ABM represents the ability of a system to resist threats, absorb shocks and recover from events. Resilience is described as an emergent property of complex systems [81, 82], and for CEES we engage with both the technical and compositional resilience of a product or engineered system structure and the functional resilience associated with its use, capabilities, and user behaviour.

ABM is defined through the specification of a simulation environment, the agents, and their interactions. Within these bounds a vast variety of configurations are possible, drawn from a variety of academic disciplines, meaning ABM lacks a widely agreed methodology. Outlined below are the key components of ABM, and approaches towards their definition (for more details see Chapter 3 in [83] and [84, 85]).

Environment

Prior to the specification of agents, the simulation environment must be defined to as a bound all individual behaviour and interaction. There are three important components to define:

- Extent (or boundary): Considering that everything cannot be modelled within our simulation, we must limit the model extents and define pathways for interaction with external systems. For example, we may wish to model specific households exposed to three types of services contract (30). Thus, we define model extents early on and take inputs from external models or data where necessary.

$$H_{Tot}(t) = \sum_{k=1}^{3} H^K(t) \tag{30}$$

1: A household population, subject to three exogenous services [86].

- Space: Simulation space may be cellular (like CA), abstract, topological, or geographic (associated with GIS data). These definitions constrain the movement of agents and placement of features.
- Time: ABMs are dynamic and progress through simulation by a particular time step referred to as a 'tick'. At each tick, agent behaviours are executed, and all simulation data updated. In modelling a real-world system, a tick must be tied to a real temporal unit, which then governs agent movement speeds. A time limit, e.g. a day, 5 years, is usually placed on the simulation.

Agents

Agents are defined through their characteristics and behaviours, which must be representative of the component subset or population of interest. In defining agents, one must balance simplicity and explainability with the level of detail required to fully elucidate the context [87, 88]. Multiple types of agents can be defined within a single ABM.

- Characteristics: The characteristics of an agent allow us to differentiate between agent types and integrate heterogeneity within agent populations. Characteristics can be assigned uniformly to subsets of agents, drawn from a random distribution or populated from evidence. Characteristics will influence decision-making, movements, and interactions with other agents.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

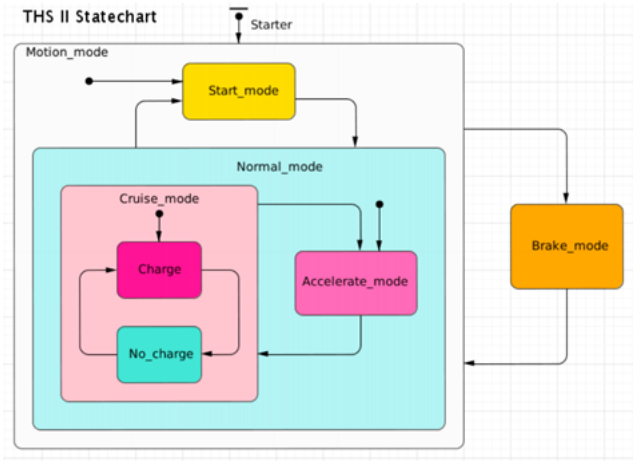


FIGURE 10: state chart for hybrid electric cars showing when charging occurs [89].

An agent, such as an organisation, when subjected to a particular threat, may have four resilience characteristics: Ability to resist, Ability to absorb, Ability to recover, and Ability to adapt to harmful events. The values of the variables representing these traits will be different for different organisations, and so when a specific organisation is subject to a simulated threat, their characteristics will determine what decisions they can make and how they can act.

- Decisions: Decisions can vary from very simple rules (e.g. always travel on the same train) to sophisticated decision-making frameworks (e.g. based on cognitive frameworks, or reinforcement learning), and result in a change of agent state. Agent decisions will be provoked by time, interaction, or changes in internal or external states, and will result in an action being taken. Agent decision models should closely reflect, or provide a reasonable representation of theoretical or observed behaviour, else results cannot be relied upon.
- Actions: Actions are responses to agent decisions and vary widely in nature, potentially including the failure or death of an agent, the movement of the agent in space (constrained by extent/boundary), interaction with nearby agents, execution of additional decision rules, consumption/depletion of available resources. The agent state may change as a result of a decision, for example, for hybrid electric vehicles, five states are possible: start, normal, accelerate, cruise and brake. The change of mode occurs as a response to a decision, such as to drive faster or to stop. Charging is constrained to cruise mode for the model in Fig. 10.

Interactions

Interactions between the agents and their environment are essential in the production of emergent properties of a system. Agent interactions may involve active exchange or occur passively through proximity alone, but will typically trigger agent decisions and actions.

- Proximity and Connectivity: In these cases, the presence or absence of other agents provokes a change in the state of an agent. Proximity is defined through spatial representation, so may relate to adjacent grid cells, topological connections, or visual observations in geographic space. Near proximity of agents may furthermore result in an interaction of competing physical forces, whereby agents are attracted or repulsed by the presence of other agents.
- Communication: Given proximity or connectivity between agents, communication may occur, whereby an agent state is influenced or changed by another agent. These communications may result in influencing decisions and actions of the agents. Communication of information between agents is a key component of agent decision making.
- Resource Exchange: Interactions may equally result in the exchange of resources, be that through cooperation (e.g. sharing of storage capacity) or competition (e.g. attempting to serve the same customers). The resulting redistribution of resources may be unconstrained, meaning a potential detriment to the wider system of interest.

The development of an ABM, and specification of the model descriptions listed above, produces a large number of parameters. Following specification of an initial model structure therefore, a secondary stage of model calibration and validation will be undertaken. This process (fully elaborated in[85, p.262] involves a) calibrating parameter settings against observed trends; and b) testing the relative effect of minor adjustments to parameter settings on system behaviour (sensitivity analysis). In general, this process will only be conducted on a few, uncertain parameters in order to limit the search space. A calibrated model should then be tested against unseen data to validate its wider suitability.

Modelling Resilience with ABM

ABM excels in its ability to represent the emergent behaviour of a system through its ability to represent the interactions between social and technical components of an engineered system [5], and expose interdependencies and fragility in their interaction [90]. ABMs can indicate the capability of a system to be resilient to threats (scenarios), the degree of failure (to provide services), the time to recover and the degree of recovered services. CEES are often too expensive or simply cannot be tested in practice against a variety of threats, and so based on the rules of behaviour and interactions between system components, an ABM can simulate and quantify the resilience of a CEES in response to attack or disruption, and the emergence of system adaptation and absorption of change.

Previous models have captured the interdependency between human and infrastructural systems in crises. As [4] demonstrated, the effect of infrastructure failure results in policy and behavioural changes that ultimately result in failures in the road and wireless phone networks. ABMs

have captured the economic and social disruption caused by power and market network failure by explicitly mapping interdependencies between systems [91, 92]. As described elsewhere (Hasan and Foliente, 2015; Rinaldi et al., 2001), ABM is broadly able to capture n-th order effects resulting from infrastructure failure. Hasan and Foliente reference the example of electric power failure, leading to gas, water, and oil supply disruption and later effects on transportation networks and the banking sector (Hasan and Foliente, 2015). Through enabling the configuration of autonomous and heterogeneous agents, be them infrastructural and human decision-makers, ABM is able to replicate interactions between critical components.

Agent-based modelling has also been applied in predicting system-level changes and response, through the actions and adaptation of its individual components. In Busch, the focus of external change was on the implementation of district heating networks, and how different intervention strategies lead to the success or failure of the policy [93]. Others have explored how ABM can realistically capture the independence and coordination of components in earthmoving operations [94, 95].

1) Case study: Electrical Power Supply System

[96] highlight the importance being placed by academia, corporations and governments on understanding system resilience and identifying ways to enhance it, especially for interdependent infrastructures on which our daily activities depend. They highlight limitations of past methods and frameworks to comprehensively assess and analyse system resilience. These limitations include tailoring to specific disruptive hazards/events, and inadequately dealing with absorption, adaptation, and recovery. They design and implement a hybrid ABM which incorporates an integrated metric to quantify system resilience. The ABM is used to simulate a specific electrical power supply system and then to quantify the improvement to resilience from alternative targeted strategies.

The key components of ABM are implemented in this model as follows:

- Environment - Extent (or boundary): Electric power supply systems (EPSS) consists of three interdependent subsystems: System Under Control (SUC) – the technical components; Operational Control System (OCS) – the control mechanisms – specifically SCADA (Supervisory Control and Data Acquisition) is used for this; and human operator level system (HOL) – the non-technical (i.e. people) parts responsible for monitoring/processing generated alarms, switching off components at remote substations and sending commands to remote substations. Environment - Space: The model is implemented using data from the real Swiss high-voltage EPSS, which consists of 219 transmission lines and 129 substations, has experienced hazards such as earthquakes and winter storms causing significant damage in at least 9 events over the past 1000 years. Environment - Time: the total power demand in a snapshot of the Swiss transmission grid on a day in winter is used. It is assumed that the disruptive event occurs at time 3 h. At t¼3 h, the disconnection of the 17 transmission lines in the selected region is triggered.
- Agents – Characteristics: Each hardware device is modeled as an agent, which maps the hardware status including operational and failures modes. Multiple devices and components exist in each layer, e.g. transmission lines (SUC), field instrumentation devices (FIDs) (OCS - SCADA), and emotion status (HOL) and each are represented by agents or objects. They have characteristics such as power flow (real number) and status (boolean). Over 1,000 individual agents appear in the model. Agents - Decisions: ABM approaches capture dynamic behaviors at the functional level. Specific behavioral rules are assigned to each agent, including both deterministic and stochastic time-dependent processes, triggered by time or inputs from other agents. E.g. a deterministic process is the power overload of a transmission line, and a stochastic process is the triggering of a component failure mode, e.g., the unplanned outage of a generator. Agents - Actions: SUC - physical and operational processes are modelled by means of DC power flow calculations. HOL - the operator acknowledges the alarm and issues the control command. HOL subtasks are sent to the "behavior" component to determine possible error modes and causes during their execution.
- Interactions - Proximity and Connectivity: The variables that define the interactions among the three subsystems act as coupling points among the three models. They are either input or output from subsystem, e.g. Status of transmission line (line connected, line disconnected) is input to SUC and HOL and output from OCS (SCADA). Interactions - Communication: The OCS (SCADA) subsystem includes various objects such as commands, alarms and monitors, whose aim is to transmit data among agents. RTU (remote terminal unit) agents (SUC) decide to whether or not to raise an alarm, and if so, it is forwarded to the relevant MTU (master terminal unit) agent. The operator (in HOL subsystem) interprets the alarm and issues a command to the MTU for related corrective actions. The MTU forwards the command to the RTU which initiates corrective action in field devices, e.g., to FCD agent to disconnect a transmission line. Interactions - Resource Exchange: The variables that define the interactions among the three subsystems act as coupling points for exchange. Power flow, and Actual load are examples of resource exchanges between agents in the SUC sub-system.
- Self-organisation: the whole system is seen to self-organise into new performance regimes with the introduction of single or combined strategies (e.g. higher RTU battery capacity improves absorptive capacity during disruption phase). The effects of enhancing the resilience of one system have a much more significant

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

impact on an interdependent system when physical dependencies are present.
- Emergence: Resilience capabilities (i.e. absorptive, adaptive and restorative capability) emerge in the model as expected and are measured although we do not know the actual form (time elapse and pattern of system performance loss) at outset. Strategies, such as storage, which delay dependency failures, are an important factor for minimizing negative effects caused by interdependencies among systems.

2) Conclusions and Limitations

ABMs like all models are simplifications of reality, albeit ABMs are the most mature tool to represent the diversity of reality including self-organisation and emergence. Representations used in models either focus on a sub-set of reality which means some aspects are ignored (outside scope) e.g. voltage magnitude is neglected in the case study; or reality is sufficiently abstracted to keep much of it in scope. Simplifications create uncertainty. The data collection need can be great especially when a specific geographical area is to be modelled. Data is needed for calibration as well as validation, and whilst methods exist to generate test data, the proximity to real world data is often uncertain. Uncertainty is usually managed by running 1000s of iterations of an ABM varying the value of variables, and usually for different scenarios (possible futures). This allows us to create a reasonable interpretation of a real system's properties but increases the computational burden. Efforts to clarify uncertainty and to assess ABM results more robustly are needed.

Researchers using ABM methods have largely addressed the need for standard frameworks to describe their models however capturing and predicting human behaviour remains challenging and relies on knowing population distributions of likely practice (which are not always Gaussian) or knowing probabilities for types of actions and responses, which are not always predictable. There is also an opportunity to hybridize ABMs as in the case study with other models to represent behaviour. More potential future directions for ABMs are listed below:

- The integration of real-time data within ABMs, via methods such as 'data assimilation', will enable the updating of simulation entities (in terms of their state, location, and behaviour) with new information. This step will ensure that agents do not diverge on unrealistic trajectories of behaviour to only be assessed as unsuccessful during model evaluation.
- The combination of modelling methodologies can improve the comprehensiveness of ABMs. This may include the improved modelling of agents via advanced machine learning (e.g. deep reinforcement learning), and the integration of ABM and other simulation methodologies to represent higher level or hierarchical processes.
- Novel approaches are required for describing and communicating uncertainty in ABM predictions. This can be achieved through simultaneous implementation of different modelling designs and assumptions via 'ensemble modelling'. Where models agree, greater certainty in future outcomes can be presented.

IV. DISCUSSION AND CONCLUSION

Three methods for uncertainty analysis in complex engineering system resilience were reviewed.

Uncertainty in Bayesian Networks is dealt with by measuring conditional probability distributions of the causal relationships among variables. The ability to model variables of several types, e.g. Boolean (yes/no), qualitative (low/medium/high), continuous, together with the ability to deal with absent data typical in the real world, makes Bayesian Networks a powerful tool for assessing engineering resilience. This can further be expanded in different scenarios, as the inland waterway port case study demonstrated. Limitations of the Bayesian Networks method are its computational cost and poor performance with very small data.

For robust Bayesian analysis of severe uncertainty, it is necessary to have a proper treatment of prior ignorance by propagating a set of prior distributions which will determine accurate inference. Imprecise Markov Chains allow us to quantify resilience of complex engineering system under severe uncertainty. The method was demonstrated on a power network and showed how statistical processes to be used in practice to reduce model discrepancies and improving risk analysis for complex engineering systems. Limitations include computational cost, and use for decision making to quantify the trade-off between cost of redundancy and resilience against common-cause failures.

Multidisciplinary Design Optimization (MDO) methods consider systems holistically by handling the flow of information among the involved disciplines and, then, the complexity of the interactions. MDO under Uncertainty (MDOU) includes reliability based multidisciplinary design optimisation (RBMDO), and robust multidisciplinary design optimisation (RMDO). MDOU for resilience requires the dynamical system to be both robust and reliable at the same time. A space systems case study addresses imprecision and epistemic uncertainty. A key issue is the need for efficient uncertainty propagation techniques in a multidisciplinary environment which deals with early stages of the design, when the number of uncertainties may be very high and their range can also be relatively broad. In this respect computationally efficient uncertainty quantification techniques must be further developed.

Three methods dealing with interconnectedness in complex engineering system resilience were reviewed.

Network science is able to fully understand cascade effects that lead to loss of resilience, by considering local functional dynamics (e.g. behaviour of a transformer) and the global topology (e.g. structure of the electricity grid) together, and give attention to the sensitivity to demand conditions and the need for tight control. This requires more processing to understand robustness and resilience than for non-engineered

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

TABLE 3: Benefits arise from each method

Method	Benefits arise from each method
Bayesian Network	• computing the posterior probability distribution of unobserved variables conditioned on some variables that have been observed, • encoding both quantitative and qualitative information in a conditional probability format. In fact, the ability to model variables of several types (e.g., variables could be Boolean (yes/no), qualitative (low/medium/high), or continuous, among others) is the main property of BN that motivates us to employ it for quantifying of system resilience.
Robust Bayesian modelling	• quantifies resilience of a complex engineering system under severe uncertainty, due to prior ignorance and/or due to lack of data, by using sets of probability distributions.
Multidisciplinary design optimization	• helps engineers in the design of systems for which the whole is greater than the sum of the parts. Several MDO methods have been developed to handle the flow of information among the involved disciplines and, then, the complexity of the interactions. • RMDO optimises the expected performance of the system and reduces at the same time the sensitivity of the optimal result to the expected uncertainties. • RbMDO optimises the expected performance and at the same time keeps the violations of the design constraints under acceptable probability thresholds. System resilience can be considered and optimised through a proper modelling of the failure modes and a formulation of the MDOU problem that explicitly takes into account the recovery time.
Networked system	• helps to fully understand networked cascade effects that lead to a loss of resilience, considers local functional dynamics and the global topology together, and gives attention to the sensitivity to demand conditions and the need for tight control. • a number of metrics can be considered, such as the time to recover from failure as well as the area under the recovery profile.
Convergent Cellular Automata	• creates built-in fault resilience and self-organising capability within complex platforms through effective detection and mitigation via triggered recovery mechanisms. • eminently compatible with existing and future configurable platforms and are essentially built upon a compromise between hardware-identical and information redundancies at the fine-grained level. • by combining CA with re-configurable information and technology platforms, new possibilities for resilience design strategies, such as self-diagnosis, self-reconfiguration and self-maintenance become available without the specific need for fault detection.
Agent based modelling	• relaxes constraints on the representation of entities, allowing for the individual representation of technical objects, subsystems, human decision-makers, and any other relevant individual actors. These entities are individual and autonomous 'agents' in ABMs and allow for the integration of distinct social and technical system components, and therefore enable a more holistic simulation of system resilience with particular relevance to complex engineered and engineering systems (CEES) that accommodate a heterogeneous population of socio-technical components. • replicates the microscopic behaviours that lead to emergence (e.g. congestion), self-organisation (e.g. autonomous re-routing), evolution (novel forms or topologies), and other properties of complex systems (e.g. repeated patterns/waves). • allows the testing of conditions under which these properties arise and dissipate in response to changes in internal or external conditions. ABM represents an ideal approach for simulating resilience, and the ability of a system to resist threats, absorb shocks and recover from events.

systems. Electricity, telecommunications, and rail transport cases are provided. Limitations focus on the relationships between topology and dynamics, the ability to faithfully represent real engineering systems, and data informing uncertainty in the parameters and inputs of the system.

By combining Cellular Automata with re-configurable information and technology platforms, new possibilities for resilience design strategies, such as self-diagnosis, self-reconfiguration and self-maintenance become available without the specific need for fault detection. Simple rules toward convergent cellular automata underpin the design of engineering systems such that desired patterns emerge from any initial configuration. A case study in electronics is considered. Limitations of convergent cellular automata include scalability, fault conditions (most effective for transient faults) and resource re-use.

Agent-based modelling (ABM) offers explicit description of autonomous and heterogeneous facets covering both technical and social components of complex engineering systems within a single integrated simulation. ABMs can quantify ability to resist threats, absorb shocks and recover from events, and models can be infinitely configurable. An electric power system is reviewed in the case study, showing the emergence of resilience capabilities (i.e. absorptive, adaptive and restorative) through self-organisation, e.g. in response to battery capacity. Limitations include the uncertainties created by simplification and data collection, as well as accurately predicting human behaviour .

Although methods contain limitations and areas for future research, those selected in this paper provide a fundamental diversity of sound approaches to assess engineering system resilience. Comparison of methods is beyond the scope of our paper, and future researchers are recommended to do this comparison. Furthermore, the potential research methodologies or any integrated approaches (i.e., integrated BN and Markov chain) that have not been used in the past but can be used as an alternative approach in the future should be considered. The case studies in this paper are only exemplars and others case studies exist.

The distinct benefits of each method in the context of resilience research study are presented in table [3]. The summary highlights the range and diversity of the methods to address uncertainty and interconnectedness in complex engineered and engineering systems.

REFERENCES

[1] Martin Mayfield, Giuliano Punzo, Richard Beasley, Ginny Clarke, Nic Holt, and Stuart Jobbins. Challenges of complexity and resilience in complex engineering systems. ENCORE Network+ White Paper, 2018.

[2] Seyedmohsen Hosseini, Kash Barker, and Jose E Ramirez-Marquez. A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145:47–61, 2016.

[3] Igor Linkov, Todd Bridges, Felix Creutzig, Jennifer Decker, Cate Fox-Lent, Wolfgang Kröger, James H Lambert, Anders Levermann, Benoit Montreuil, Jatin Nathwani, et al. Changing the resilience paradigm. Nature Climate Change, 4(6):407, 2014.

[4] Chris Barrett, Richard Beckman, Karthik Channakeshava, Fei Huang, VS Anil Kumar, Achla Marathe, Madhav V Marathe, and Guanhong Pei. Cascading failures in multiple infrastructures: From transportation to communication network. In 2010 5th International Conference on Critical Infrastructure (CRIS), pages 1–8. IEEE, 2010.

[5] Koen H Van Dam, Igor Nikolic, and Zofia Lukszo. Agent-based modelling of socio-technical systems, volume 9. Springer Science & Business Media, 2012.

[6] Edward Crawley, Olivier De Weck, Christopher Magee, Joel Moses, Warren Seering, Joel Schindall, David Wallace, Daniel Whitney, et al. The influence of architecture in engineering systems (monograph. MIT Engineering System Symposium, 2004.

[7] Seyedmohsen Hosseini and Kash Barker. Modeling infrastructure resilience using bayesian networks: A case study of inland waterway ports. Computers & Industrial Engineering, 93:252–266, 2016.

[8] Seyedmohsen Hosseini, Nita Yodo, and Pingfeng Wang. Resilience modeling and quantification for design of complex engineered systems using bayesian networks. In ASME 2014 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, pages V02AT03A040–V02AT03A040. American Society of Mechanical Engineers, 2014.

[9] Seyedmohsen Hosseini and Kash Barker. A bayesian network model for resilience-based supplier selection. International Journal of Production Economics, 180: 68–87, 2016.

[10] Riska Asriana Sutrisnowati, Hyerim Bae, and Minseok Song. Bayesian network construction from event log for lateness analysis in port logistics. Computers & Industrial Engineering, 89:53–66, 2015.

[11] Golam Kabir, Solomon Tesfamariam, Alex Francisque, and Rehan Sadiq. Evaluating risk of water mains failure using a bayesian belief network model. European Journal of Operational Research, 240(1):220–234, 2015.

[12] Nima Khakzad. Application of dynamic bayesian network to risk analysis of domino effects in chemical infrastructures. Reliability Engineering & System Safety, 138:263–272, 2015.

[13] Peter Morris, Desley Vine, and Laurie Buys. Application of a bayesian network complex system model to a successful community electricity demand reduction program. Energy, 84:63–74, 2015.

[14] Seyedmohsen Hosseini, Dmitry Ivanov, and Alexandre Dolgui. Ripple effect modelling of supplier disruption: integrated markov chain and dynamic bayesian network approach. International Journal of Production Research, pages 1–19, 2019.

[15] Cameron A MacKenzie, Kash Barker, and F Hank Grant. Evaluating the consequences of an inland waterway port closure with a dynamic multiregional interdependence model. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 42 (2):359–370, 2012.

[16] Norman Fenton, Martin Neil, and David A Lagnado. A general structure for legal arguments about evidence using bayesian networks. Cognitive science, 37(1):61–102, 2013.

[17] Seyedmohsen Hosseini and Dmitry Ivanov. A new resilience measure for supply networks with the ripple effect considerations: a bayesian network approach. Annals of Operations Research, pages 1–27, 2019.

[18] Pierre Simon Laplace. Essai philosophique sur les probabilitiés. Bachelier, Paris, 1825. Cinquième édition.

[19] Jose M. Bernado and Adrian F. M. Smith. Bayesian Theory. John Wiley and Sons, 1994.

[20] George Boole. An investigation of the laws of thought on which are founded the mathematical theories of logic and probabilities. Walton and Maberly, London, 1854.

[21] Peter Walley. Statistical Reasoning with Imprecise Probabilities. Chapman and Hall, London, 1991.

[22] James O. Berger. The robust Bayesian viewpoint. In J. B. Kadane, editor, Robustness of Bayesian Analyses, pages 63–144. Elsevier Science, Amsterdam, 1984.

[23] Roy Billinton and Ronald N. Allan. Reliability Evaluation of Engineering Systems: Concepts and Techniques. Plenum Press, 2nd edition, 1992.

[24] A. A. Markov. Primer statisticheskogo issledovaniya nad tekstom “Evgeniya Onegina”, illyustriruyuschij svyaz’ ispytanij v cep’. Izvestija Imp. Akad. nauk, SPb, VI seriya(3):153–162, 1913.

[25] Damjan Škulj. Efficient computation of the bounds of continuous time imprecise Markov chains. Applied Mathematics and Computation, 250:165–180, 2015. .

[26] Matthias C. M. Troffaes, Dana L. Kelly, and Gero Walter. Imprecise Dirichlet model for common-cause failure. In 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012), pages 6722–6728, June 2012. ISBN 978-1-62276-436-5.

[27] Matthias C. M. Troffaes and Simon Blake. A robust data driven approach to quantifying common-

cause failure in power networks. In F. Cozman, T. Denœux, S. Destercke, and T. Seidenfeld, editors, ISIPTA'13: Proceedings of the Eighth International Symposium on Imprecise Probability: Theories and Applications, pages 311–317, Compiègne, France, July 2013. SIPTA. URL http://www.sipta.org/isipta13/index.php?id=paper&paper=031.html.

[28] Matthias C. M. Troffaes, Gero Walter, and Dana Kelly. A robust Bayesian approach to modelling epistemic uncertainty in common-cause failure models. Reliability Engineering and System Safety, 125:13–21, May 2014. . Special issue of selected articles from ESREL 2012.

[29] Matthias Troffaes, Jacob Gledhill, Damjan Škulj, and Simon Blake. Using imprecise continuous time Markov chains for assessing the reliability of power networks with common cause failure and non-immediate repair. In Thomas Augustin, Serena Doria, Enrique Miranda, and Erik Quaeghebeur, editors, ISIPTA'15: Proceedings of the 9th International Symposium on Imprecise Probability: Theories and Applications, pages 287–294, Pescara, Italy, July 2015. ARACNE. ISBN 978-88-548-8555-4. URL http://www.sipta.org/isipta15/data/paper/18.pdf.

[30] Simon Blake and Philip Taylor. Handbook of Power Systems II, chapter Aspects of Risk Assessment in Distribution System Asset Management: Case Studies, pages 449–480. Springer, 2010. ISBN 978-3-642-12685-7.

[31] Simon Blake, Philip Taylor, and David Miller. A composite methodology for evaluating network risk. In CIRED 21st International Conference on Electricity Distribution, Frankfurt, Germany, June 2011.

[32] A. Mosleh, K. N. Fleming, G. W. Parry, H. M. Paula, D. H. Worledge, and D. M. Rasmuson. Procedures for treating common cause failures in safety and reliability studies: Procedural framework and examples. Technical Report NUREG/CR-4780, PLG Inc., Newport Beach, CA (USA), January 1988.

[33] Matthias C. M. Troffaes. Decision making under uncertainty using imprecise probabilities. International Journal of Approximate Reasoning, 45(1):17–29, May 2007. .

[34] Joaquim R. R. A. Martins and Andrew B. Lambe. Multidisciplinary design optimization: A survey of architectures. AIAA Journal, 51(9):2049–2075, 2017/09/19 2013. . URL https://doi.org/10.2514/1.J051895.

[35] Wen Yao, Xiaoqian Chen, Wencai Luo, Michel van Tooren, and Jian Guo. Review of uncertainty-based multidisciplinary design optimization methods for aerospace vehicles. Progress in Aerospace Sciences, 47(6):450 – 479, 2011. ISSN 0376-0421.

[36] J.C. Helton. Uncertainty and sensitivity analysis in the presence of stochastic and subjective uncertainty. Journal of Statistical Computation and Simulation, 57: 3–76, 1997.

[37] M. Vasile and S. Alicino. Evidence-based preliminary design of spacecraft. In 6th International Conference on Systems & Concurrent Engineering for Space Applications. SECESA 2014. SECESA 2014, 2014.

[38] M. Vasile, G. Filippi, C. Ortega, and A. Riccardi. Fast belief estimation in evidence network models. In EUROGEN 2017, 2017.

[39] M. Vasile. On the solution of min-max problems in robust optimisation. In The EVOLVE, 2014.

[40] M. Di Carlo, M. Vasile, and E. Minisci. Multi-population inflationary differential evolution algorithm with adaptive local restart. In IEEE Congress on Evolutionary Computation (CEC), 2015.

[41] G. Filippi, M. Vasile, M. Bianchi, and P. Vercesi. Evidence-based robust optimisation of space systems with evidence network models. In 2018 IEEE Congress on Evolutionary Computation (CEC). IAAA CEC 2018, 2018.

[42] J.F. Castet and J.H. Saleh. Satellite and satellite subsystems reliability: Statistical data analysis and modeling. Reliability Engineering and System Safety, 94(11),: 1718–1728, 2009.

[43] J.F. Castet and J.H. Saleh. Beyond reliability, multi-state failure analysis of satellite subsystems: a statistical approach. Reliability Engineering and System Safety, 95(4):311–322, 2010.

[44] G. Filippi, D. Krpelik, P. Zeno Korondi, M. Vasile, M. Marchi, and C. Poloni. Systems resilience engineering and global system reliability optimisation underimprecision and epistemic uncertainty. In 69th International Astronautical Congress, 69thInternational Astronautical Congress (IAC), Bremen, Germany, 2018.

[45] L. Brevault, M. Balesdent, N. Bérend, and R. Le Riche. Challenges and future trends in uncertainty-based multidisciplinary design optimization for space transportation system design. In 5th EUROPEAN CONFERENCE FOR AEROSPACE SCIENCES (EUCASS), Munich, Germany, 1-5 July 2013.

[46] M. Newman. Networks. Oxford University Press, 2018.

[47] R. May. Will a large complex system be stable? Nature, 238, 1972.

[48] S. Johnson, V. Garcia, L. Donetti, and M. Munoz. Trophic coherence determines food-web stability. Proc. Nat. Academy of Sciences (PNAS), 111, 2014.

[49] A. Ma and R. Mondragon. Rich-Cores in Networks. PLOS ONE, 10, 2015.

[50] C. Lv, S. Si, D. Duan, and R. Zhan. Dynamical robustness of networks against multi-node attacked. Physica A: Stat. Mechanics and its Applications, 471, 2017.

[51] G. Moutsinas and W. Guo. Node-Level Resilience Loss in Dynamic Complex Networks. preprint on arXiv, 2018.

[52] J. Gao, B. Barzel, and A. Barabasi. Universal resilience patterns in complex networks. Nature, 530, 2016.

[53] J. Nitzbon, P. Schultz, J. Heitzig, J. Kurths, and F. Hellmann. Deciphering the imprint of topology on nonlinear dynamical network stability. New Journal of

Physics, 19, 2017.

[54] B. Schafer, D. Witthaut, M. Timme, and Vito Latora. Dynamically induced cascading failures in power grids. Nature Communication, 2018.

[55] R. Zimmerman, C. Murillo-Sanchez, and J. Thomas. Steady-state Operations, Planning, and Analysis Tools for Power Systems Research and Education. IEEE Transactions on Power Systems, 26, 2011.

[56] C. Saha, M. Afshang, and H. Dhillon. 3GPP-Inspired HetNet Model Using Poisson Cluster Process: Sum-Product Functionals and Downlink Coverage. IEEE Transactions on Communications, 66(5), 2018.

[57] H. Feyzmahdavian, M. Johansson, and T. Charalambous. Contractive Interference Functions and Rates of Convergence of Distributed Power Control Laws. IEEE Transactions on Wireless Communications, 11 (12), 2012.

[58] W. Guo and T. O'Farrell. Dynamic Cell Expansion with Self-Organizing Cooperation. IEEE Journal on Selected Areas in Communications (JSAC), 31, 2013.

[59] A. Pagani, G. Mosquera, A. Alturki, S. Johnson, S. Jarvis, A. Wilson, W. Guo, and L. Varga. Resilience or Robustness: Identifying Topological Vulnerabilities in Rail Networks. Royal Society Open Science, 2019.

[60] J. Liang, Y. Hu, G. Chen, and T. Zhou. A universal indicator of critical state transitions in noisy complex networked systems. Scientific Reports, 7, 2017.

[61] Zhuangkun Wei, Bin Li, and Weisi Guo. Optimal sampling in joint time- and graph-domains for dynamic complex networks. IEEE Trans. on Sig. and Info. Proc. (to appear), 2019.

[62] X. Liu, L. Pan, H. Stanley, and J. Gao. Controllability of giant connected components in a directed network. Physical Review E, 95, 2017.

[63] M.G. Parris, C.A. Sharma, and R.F. Demara. Progress in Autonomous Fault Recovery of Field Programmable Gate Arrays. ACM Comput. Surv., 43(4):31:1–31:30, October 2011.

[64] J.A. Cheatham, J.M. Emmert, and S. Baumgart. A survey of fault tolerant methodologies for FPGAs. ACM Trans. Des. Autom. Electron. Syst., 11(2):501–533, April 2006.

[65] J. Von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. Automata studies, 34:43–98, 1956.

[66] W. Jiang, C. Hu, Y. Zhou, and A. Kanevsky. Are Disks the Dominant Contributor for Storage Failures?: A Comprehensive Study of Storage Subsystem Failure Characteristics. Trans. Storage, 4(3):7:1–7:25, November 2008.

[67] H.V. Allen, S.C. Terry, and D.W. De Bruin. Accelerometer systems with self-testable features. Sensors and Actuators, 20(1):153–161, 1989.

[68] M.A. Trefzer and A.M. Tyrrell. Evolvable Hardware: From Practice to Application. Natural Computing Series. Springer Berlin Heidelberg, 2016.

[69] R. McWilliam, P. Schiefer, and A. Purvis. Building Dependable Electronic Systems for Autonomous Maintenance, pages 375–394. Springer International Publishing, 2015.

[70] J. Qingwei. Write Fault Protection Against Shock Disturbance in Hard Disk Drives Without a Shock Sensor. IEEE Transactions on Magnetics, 43(9):3689–3693, September 2007.

[71] R. Barzel. A structured approach to physically-based modeling. Academic Press, Cambridge MA, 1992.

[72] P. Eggenberger. Evolving morphologies of simulated 3d organisms based on differential gene expression. Proceedings of the 4th European Conference on Artificial Life, 1997.

[73] Ch. Mizas, G.Ch. Sirakoulisa, V. Mardirisa, I. Karafyllidis, N. Glykosb, and R. Sandaltzopoulos. Reconstruction of dna sequences using genetic algorithms and cellular automata:next term towards mutation prediction? Journal of theoretical biology, 92:61–68, 2008.

[74] J. Miller. Principles in the evolutionary design of digital circuits, part 1. Journal of genetic programming and evolvable machines, 1(1), 2000.

[75] J.F. Miller and W. Banzhaf. Evolving the program for a cell: From french flags to boolean circuits. On Growh, Form and Computers, 2003.

[76] H. Liu, J.F. Miller, and A.M. Tyrrell. An intrinsic robust transient fault-tolerant developmental model for digital systems. In Workshop on Regeneration and Learning in Developmental Systems, Genetic and Evolutionary Computation Conference, 2004.

[77] R. McWilliam, S. Philipp, and A. Purvis. Creating self-configuring logic with built-in resilience to multiple-upset events. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, 2015.

[78] D.H Jones, R. McWilliam, and A Purvis. Mimicking morphogenesis for robust behaviour of cellular architectures. In World Academy of Science, Engineering and Technology International Conference on Biosciences and Bioengineering 2008, pages 59–61, 2008.

[79] David Huw Jones, Alan Purvis, and Richard McWilliam. Design of self-assembling, self-repairing 3d irregular cellular automata, 2011.

[80] D.H. Jones, R. McWilliam, and A. Purvis. Convergence and feedback: A framework for bounded cellular automata design. Journal of Cellular Automata, 6, 2011.

[81] Michael Batty. The new science of cities. MIT press, 2013.

[82] Volker Grimm and Justin M Calabrese. What is resilience? a short introduction. dans viability and resilience of complex systems (pp. 3–13), 2011.

[83] Andrew Crooks, Nicolas Malleson, Ed Manley, and Alison Heppenstall. Agent-Based Modelling and Geographical Information Systems: A Practical Primer. SAGE Publications Limited, 2018.

[84] Uri Wilensky and William Rand. An introduction to

agent-based modeling: modeling natural, social, and engineered complex systems with NetLogo. MIT Press, 2015.

[85] Volker Grimm and SF Railsback. Agent-based and individual-based modeling: a practical introduction. Princeton University Press Princeton, NJ, 2011.

[86] Marguerite Robinson, Liz Varga, and Peter Allen. An agent-based model for energy service companies. Energy conversion and management, 94:233–244, 2015.

[87] Robert Axelrod. The complexity of cooperation: Agent-based models of competition and collaboration, volume 3. Princeton University Press, 1997.

[88] Bruce Edmonds and Scott Moss. From kiss to kids–an 'anti-simplistic' modelling approach. In International workshop on multi-agent systems and agent-based simulation, pages 130–144. Springer, 2004.

[89] José María Gonzalez de Durana, Oscar Barambones, Enrique Kremers, and Liz Varga. Agent-based modeling of the energy network for hybrid cars. Energy conversion and management, 98:376–386, 2015.

[90] Steven M Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the, pages 8–pp. IEEE, 2004.

[91] Dianne C Barton, Eric D Eidson, David A Schoenwald, Kevin L Stamber, and Rhonda K Reinert. Aspen-ee: an agent-based model of infrastructure interdependency. SAND2000-2925. Albuquerque, NM: Sandia National Laboratories, 2000.

[92] Dianne C Barton, Eric D Edison, David A Schoenwald, Roger G Cox, and Rhonda K Reinert. Simulating economic effects of disruptions in the telecommunications infrastructure. Sandia Report, SAND2004-0101, 2004.

[93] Jonathan Busch, Katy Roelich, Catherine SE Bale, and Christof Knoeri. Scaling up local energy infrastructure; an agent-based model of the emergence of district heating networks. Energy policy, 100:170–180, 2017.

[94] Ahmad Jabri and Tarek Zayed. Agent-based modeling and simulation of earthmoving operations. Automation in Construction, 81:210–223, 2017.

[95] Faridaddin Vahdatikhaki, Seied Mohammad Langari, Alhusain Taher, Khaled El Ammari, and Amin Hammad. Enhancing coordination and safety of earthwork equipment operations using multi-agent system. Automation in construction, 81:267–285, 2017.

[96] Cen Nan and Giovanni Sansavini. A quantitative method for assessing resilience of interdependent infrastructures. Reliability Engineering & System Safety, 157:35–53, 2017.

S. NEDA NAGHSHBANDI is a PhD candidate at University College London, UK, studying "decentralized adaptive multi-agent collaboration for resilient earthmoving operation" . She received a Master degree of Construction Project Management from Heriot-Watt University, Scotland, UK (2012). She also has a Bachelor degree in Civil Engineering from the University of Kurdistan, Iran (2010).

During her PhD studies, she has been involved in a number of research projects in the areas of complex systems, emergent behaviour, engineered and engineering system resilience including infrastructure resilience, and connected autonomous plant.

LIZ VARGA received her Ph.D. degree from Cranfield University, Bedford, UK. She also has an MBA from Cranfield and a first class honours degree from the Open University, Milton Keynes, UK. Prof Varga has a chair in Complex Systems at University College London (UCL), London, UK (2018-) and was previously Professor of Complex Infrastructure Systems at Cranfield University (2015-19).

She leads the Infrastructure Systems Institute (UCL) and is section head for Infrastructure and Cities in the Civil, Environmental, Geomatics Engineering Department (UCL). She has published over 60 journal papers on infrastructure systems: energy, transport, water, waste and telecommunications, including Energy and Complexity: New Ways Forward Applied Energy (2015) 138 (1) 150-159. She is a regular speaker, reviewer and advisor on infrastructure matters.

Prof Varga is a fellow of the Higher Education Academy and was awarded the Research Prize (Cranfield University) (2014, 2016). She led an international satellite workshop on Integrated Utility Services at the international European Complex Systems Conference (ECCS), Barcelona, Spain, Sep 2013, which led to a special issue of Emergence: Complexity and Organisation (E:CO) journal.

ALAN PURVIS (MIEEE'12, LMIEEE'19) was born in Gateshead, County Durham,UK in 1954. He received his BSc Degree from Leeds University, Leeds, West Yorkshire, UK in 1976, and the PhD degree from Cambridge University, Cambridgeshire, UK in 1981.

He was a PostDoctoral Fellow at Cambridge University, UK in 1981 at the Cavendish Laboratory. He joined the Physics Department at Durham University, Durham and then was appointed as Lecturer in the School of Engineering and Applied Sciences at of Durham University, then Reader and then Full Professor in 1995 where he specialised in resilient electronics and the detection of weak signals in noise. At present he is an Emeritus Professor in the Department of Engineering at Durham University.

Alan is a Fellow of the Institution of Electronics and Technicians, IET, UK and a Chartered Engineer, CEng, UK.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

RICHARD MCWILLIAM was born in Keith, United Kingdom, in 1977. He received the M.Eng. degree in electronic and electrical engineering from Aberdeen University, United Kingdom in 1999, and the Ph.D. in electronic engineering from Durham University, United Kingdom, in 2003.

From 2003 to 2011 he was postdoctoral associate at Durham University, United Kingdom, where he engaged in research on computer-generated holography for photolithography. From 2011 to 2016 he joined the Centre for Through-life Engineering Services, Cranfield University, United Kingdom working on self-repair strategies for electronic systems. He is currently Senior Scientist at IBEX Innovations, Sedgefield, United Kingdom, working in the area of machine learning and image processing for X-ray imaging.

EDMONDO MINISCI earned his Bachelor's degree in Aerospace Engineering at Politecnico di Torino in 1998 and his Ph.D. in Aerospace Engineering at Politecnico di Torino in 2004. He is a senior Lecturer in Multi-Disciplinary Design Optimisation at the Department of Mechanical & Aerospace Engineering of University of Strathclyde.

He is the director of the Intelligent Computational Engineering Laboratory (ICE-Lab) and I have 15+ years of experience in the field of model based analysis and design optimisation of complex mechanical systems/devices. He is also founder member and former general manager of OPTIMAD Engineering S.r.l. – Italian SME, Spin-off of the Politecnico di Torino, active in the field of aerodynamic analysis, design, and optimization.

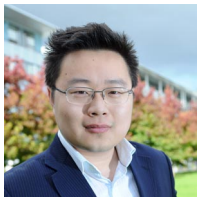
MASSIMILIANO VASILE received the M.S. and Ph.D. degrees from the Politecnico di Milano, Milan, Italy, in 1996 and 2001, respectively. He is a Professor of Space Systems Engineering, and Director of the Aerospace Centre of Excellence in the Department of Mechanical and Aerospace Engineering, University of Strathclyde, Glasgow, U.K. Prior to this, from 2005 to 2010, he was Head of Research with the Space Advanced Research Team, University of Glasgow, Glasgow, U.K. Before starting his academic career in 2004, he was the First Member of the ESA Advanced Concepts Team and initiator of the ACT research streams. His research interests include astrodynamics, space traffic management, computational intelligence and optimization under uncertainty. Prof. Vasile is a member of the IAF Astrodynamics and Space Power Committee, the IEEE Committee on Emerging Technologies in Computational Intelligence, and theUNSpace Mission Planning Advisory Group. He is a Senior Member of the American Institute of Aeronautics and Astronautics.

MATTHIAS TROFFAES was born in Brugge, Belgium, in 1977. He received the M.Eng. degree in theoretical physics from Gent University, Gent, Belgium, in 2000, the B.Sc. degree in music (harpsichord) from the Royal Conservatory, Gent, Belgium, in 2001, and the Ph.D. degree in applied sciences from Gent University, Gent, Belgium, in 2005.

From 2005 to 2006, he visited Carnegie Mellon University, Pittsburgh, PA, USA, as a Francqui Foundation Fellow of the Belgian American Educational Foundation, working as a post-doctoral researcher. He joined Durham University, Durham, UK, in 2006, where he is currently a Professor of probability. His research is concerned with probabilistic methods for modelling and quantifying severe uncertainty and decision making under severe uncertainty, the theoretical foundations behind such modelling, and practical statistical applications thereof, mostly in engineering and in environmental sciences. He is the author numerous published articles, as well as the book "Lower Previsions" (Wiley, 2014) jointly written with Gert De Cooman.

Prof. Troffaes has been a member of the executive committee of SIPTA (The Society for Imprecise Probability: Theories and Applications) since 2009, acting as president of the society from 2015 to 2017. He is also a Fellow of the Higher Education Academy.

TABASSOM SEDIGHI gained her BSc in Physics and undertook her MSc in Control Engineering (Coventry University, UK). She received her PhD at Cranfield University as part of the No Fault Found (NFF) project sponsored by EPSRC and BAE systems, United Kingdom. Currently, she is a research fellow in Soil informatics Centre for Environment and Agricultural Informatics, Cranfield University. She has been actively involved in the NFF project regarding the intermittent fault detection and prediction of test facilities for assessment of intermittent fault patterns and deployment statistical methods (Dynamic Bayesian Network, Gaussian process, etc.) for intermittent fault prediction.



WEISI GUO (S'07-M'11-SM'17) received his combined BEng and MEng, MA, and PhD from the University of Cambridge in 2005 and 2011 respectively. From 2005-2007, he was a 2G/3G radio engineer at T-Mobile International. From 2010-12 he was an EPSRC post-doctoral research associate at Swansea University and University of Sheffield. From 2012-17 he was an assistant and then associate professor at the University of Warwick. He also held an Alan Turing Fellowship from 2017-19. From 2019, he is now Chair Professor of Human Machine Intelligence at Cranfield University, where he leads research in trustworthy AI and algorithms for infrastructure wireless sensing and optimisation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992239, IEEE Access

ED MANLEY Ed Manley was born in Reading, United Kingdom in 1982. He received a BSc from University of East Anglia, MSc from University of Leeds, and an MRes and EngD from University College London. He was a Research Associate at the Bartlett Centre for Advanced Spatial Analysis (CASA), University College London, from 2013 to 2014, before taking a Lecturer position in the same department. He was promoted to Associate Professor in 2018, and served as departmental Director of Research during this time. He moved to University of Leeds as Professor in Urban Analytics in 2019. He is author of the book 'Agent-based Modelling and Geographical Information Science', published by Sage in 2018. Prof. Manley is a Fellow of the Royal Geographical Society and Royal Society of Arts (RSA).

DAVID H. JONES was born in Leamington Spa, UK in 1983. He received the MEng in electronic engineering from the University of York in 2005, the Ph.D. degree in electronic engineering from Durham University in 2008. From 2008 to 2011 he was a research associate at Imperial College London. From 2011-2015 he was with the British Antarctic Survey airborne survey division. From 2015-2016 he was a lecturer at Coventry University. He is currently Chief of Engineering at MDA Space and Robotics. His research has been concerned with high reliability engineering, robust sensor design and high performance computing.